(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平10－247905

(43)公開日　平成10年(1998)９月14日

(51)Int.Cl.[6]		識別記号	FI		
Ｈ０４Ｌ	9/32		Ｈ０４Ｌ	9/00	６７５Ｂ
Ｇ０６Ｆ	1/00	３７０	Ｇ０６Ｆ	1/00	３７０Ｅ
	9/06	５５０		9/06	５５０Ｅ
					５５０Ｃ
					５５０Ｋ

審査請求　未請求　請求項の数51　ＯＬ　（全 49 頁）　最終頁に続く

(21)出願番号　特願平9－38770

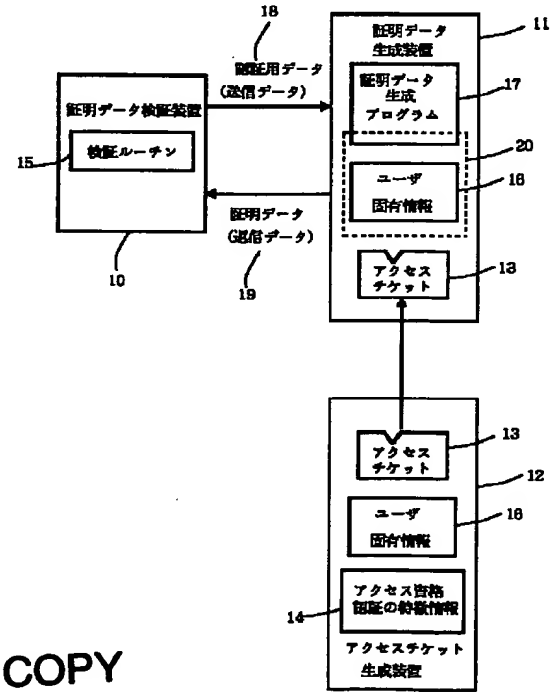
(22)出願日　平成９年(1997)２月24日

(31)優先権主張番号　特願平8－62076
(32)優先日　平８(1996)２月23日
(33)優先権主張国　日本（ＪＰ）
(31)優先権主張番号　特願平9－418
(32)優先日　平９(1997)１月６日
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000005496
富士ゼロックス株式会社
東京都港区赤坂二丁目17番22号
(72)発明者　申　吉浩
神奈川県足柄上郡中井町境430　グリーンテクなかい　富士ゼロックス株式会社内
(72)発明者　小林　健一
神奈川県足柄上郡中井町境430　グリーンテクなかい　富士ゼロックス株式会社内
(72)発明者　荒谷　徹
神奈川県足柄上郡中井町境430　グリーンテクなかい　富士ゼロックス株式会社内
(74)代理人　弁理士　澤田　俊夫

(54)【発明の名称】　アクセス資格認証装置および方法

(57)【要約】
【課題】　多数の認証鍵等の固有情報を取り扱うことから派生する負担を、ユーザ側およびアプリケーション作成者等のプロテクト側の双方から解消する。
【解決手段】　アクセスチケット生成装置１２がユーザ固有情報およびアクセス資格認証の特徴情報からアクセスチケットを生成する。ユーザの証明データ生成装置１１はアクセスチケットを受領し、証明データ検証装置１０から受信した認証用データを、アクセスチケットおよびユーザ固有情報を用いて証明データに変換し、証明データ検証装置１０に返信する。証明データ検証装置１０は証明データを自ら保持する期待値等を用いて検証する。



【特許請求の範囲】
【請求項１】　ユーザのアクセス資格を証明するために生成された証明データの正当性を検証することにより上記ユーザのアクセス資格を認証するアクセス資格認証装置において、
認証用データを記憶する第１の記憶手段と、
ユーザの固有情報を記憶する第２の記憶手段と、
上記ユーザの固有情報と、アクセス資格認証の特徴情報とに対し、所定の計算を実行した実行結果である証明用補助情報を記憶する第３の記憶手段と、
上記第１の記憶手段に保持されている認証用データと、上記第２の記憶手段に記憶されている上記ユーザの固有情報と、上記第３の記憶手段に記憶されている上記証明用補助情報とに所定の計算を施して証明データを生成する証明データ生成手段と、
上記証明データ生成手段によって生成された証明データが上記アクセス資格認証の特徴情報に基づいて生成されていることを検証する証明データ検証手段とを有することを特徴とするアクセス資格認証装置。
【請求項２】　少なくとも、上記第２の記憶手段と、上記証明データ生成手段とが、内部のデータ及び処理手続を外部から観測することを困難ならしめる防御手段中に保持されていることを特徴とする請求項１記載のアクセス資格認証装置。
【請求項３】　少なくとも、上記第２の記憶手段と、上記証明データ生成手段とが、ＩＣカードなどの携帯可能な小型演算装置として構成されていることを特徴とする請求項１記載のアクセス資格認証装置。
【請求項４】　上記証明データ生成手段が、第１の演算手段と、第２の演算手段とから構成され、
第１の演算手段は、上記第２の記憶手段に記憶されているユーザの固有情報と、上記第３の記憶手段に記憶されている証明用補助情報とに所定の計算を施し、その結果として上記アクセス資格認証の特徴情報を算出し、
第２の演算手段は、上記第１の記憶手段に記憶されている認証用データと、第１の演算手段によって算出されたアクセス資格認証の特徴情報とに所定の計算を施し、その結果として上記証明データを生成することを特徴とする請求項１乃至３記載のアクセス資格認証装置。
【請求項５】　上記証明データ生成手段が、第３の演算手段と、第４の演算手段と、第５の演算手段とから構成され、
第３の演算手段は、上記第１の記憶手段に記憶されている認証用データと、上記第３の記憶手段に記憶されている証明用補助情報とに所定の計算を施し、
第４の演算手段は、上記第１の記憶手段に記憶されている認証用データと、第２の記憶手段に記憶されているユーザの固有情報とに所定の計算を施し、
第５の演算手段が、上記第３の演算手段による計算結果と、上記第４の演算手段による計算結果とに所定の計算を施し、その結果として上記証明データを生成することを特徴とする請求項１乃至３記載のアクセス資格認証装置。
【請求項６】　少なくとも、上記第２の記憶手段と、上記第４の演算手段とが、内部のデータ及び処理手続を外部から観測することを困難ならしめる防御手段中に保持されていることを特徴とする請求項５に記載のアクセス資格認証装置。
【請求項７】　少なくとも、上記第２の記憶手段と、上記第４の演算手段とが、ＩＣカードなどの携帯可能な小型演算装置として構成されていることを特徴とする請求項５に記載のアクセス資格認証装置。
【請求項８】　上記アクセス資格認証の特徴情報が暗号関数における復号鍵であり、上記認証用データが適当なデータを前記復号鍵に対応する暗号化鍵を用いて暗号化したものであり、
上記証明データ検証手段は、上記証明データ生成手段が生成する上記証明データが認証用データを正しく復号したものであることを検証することを特徴とする請求項１乃至７に記載のアクセス資格認証装置。
【請求項９】　上記アクセス資格認証の特徴情報が暗号関数における暗号化鍵であり、上記証明データ生成手段が生成する上記証明データが上記認証用データを前記暗号化鍵を用いて正しく暗号化したものであることを検証することを特徴とする請求項１乃至７に記載のアクセス資格認証装置。
【請求項１０】　上記アクセス資格認証の特徴情報がデジタル署名関数における署名鍵であり、上記証明データ生成手段が生成する上記証明データが、上記認証用データに対して、前記署名鍵を用いて正しく生成されたデジタル署名であることを検証することを特徴とする請求項１乃至７に記載のアクセス資格認証装置。
【請求項１１】　暗号化関数が非対称鍵暗号関数であり、アクセス資格認証の特徴情報が鍵の一方であることを特徴とする請求項８または９に記載のアクセス資格認証装置。
【請求項１２】　暗号化関数が公開鍵暗号関数であり、アクセス資格認証の特徴情報が秘密鍵であることを特徴とする請求項１１に記載のアクセス資格認証装置。
【請求項１３】　暗号化関数が対称鍵暗号関数であり、アクセス資格認証の特徴情報が共通秘密鍵であることを特徴とする請求項８または９に記載のアクセス資格認証装置。
【請求項１４】　上記第１の記憶手段と、上記第２の記憶手段と、上記第３の記憶手段と、上記証明データ生成手段とから構成される証明データ生成装置と、
上記証明データ検証手段に加え、認証用データを記憶する第４の記憶手段と、証明データを記憶する第５の記憶手段を備えた証明データ検証装置とが、互いに通信することによりユーザのアクセス資格を認証するアクセス資

格認証装置において、
証明データ検証装置は、第４の記憶手段に記憶されている認証用データを証明データ生成装置の第１の記憶手段に書き出し、
証明データ生成装置は、証明データ生成手段によって第１の記憶手段に書き込まれた上記認証用データをもとに生成した証明データを、証明データ検証装置中の第５の記憶手段に書き出し、
証明データ検証装置は第５の記憶手段に書き込まれた上記証明データを用いてユーザのアクセス資格を認証することを特徴する請求項１乃至１３に記載のアクセス資格認証装置。
【請求項１５】　上記アクセス資格認証の特徴情報が暗号化関数の暗号化鍵であり、
証明データ検証装置が乱数生成手段を備え、乱数生成手段は生成した乱数を認証用データとして第４の記憶手段に書き込み、
証明データ検証手段は、証明データ生成装置によって第５の記憶手段に書き込まれた証明データが前記乱数である認証用データをアクセス資格認証の特徴情報である暗号化鍵で暗号化したものであることを検証することを特徴とする請求項１４に記載のアクセス資格認証装置。
【請求項１６】　アクセス資格認証の特徴情報が暗号化関数の復号鍵であり、
証明データ検証装置が乱数生成手段と、生成した乱数を記憶する第６の記憶手段と、認証用素データを記憶する第７の記憶手段とを備え、
乱数生成手段は生成した乱数を第６の記憶手段に書き込むと共に、第７の記憶手段に記憶されている認証用素データに前記乱数を用いた乱数効果を施した後、認証用データとして第４の記憶手段に書き込み、
証明データ検証手段は、第６の記憶手段に記憶されている乱数による乱数効果を、上記証明データ生成装置によって第５の記憶手段に書き込まれた証明データから除去した結果が、アクセス資格認証の特徴情報である復号鍵で第７の記憶手段に記憶されている認証用素データを復号したものであることを検証することを特徴とする請求項１４に記載のアクセス資格認証装置。
【請求項１７】　上記アクセス資格認証の特徴情報がデジタル署名関数の署名鍵であり、
証明データ検証装置が乱数生成手段を備え、乱数生成手段は生成した乱数を認証用データとして第４の記憶手段に書き込み、
証明データ検証手段は、証明データ生成装置によって第５の記憶手段に書き込まれた証明データが、前記乱数である認証用データに対する、アクセス資格認証の特徴情報である署名鍵によるデジタル署名であることを検証することを特徴とする請求項１４に記載のアクセス資格認証装置。
【請求項１８】　暗号化関数が法ｎのもとでのＲＳＡ公開鍵暗号であり、アクセス資格認証の特徴情報が秘密鍵Ｄであり、秘密鍵Ｄに対応する公開鍵がＥであり、
証明データ検証手段は、第５の記憶手段に書き込まれた証明データＲをＥ乗した結果と、第４の記憶手段に記憶されている認証用データＣとが、法ｎのもとで合同であること（$R^E \mod n = C \mod n$）を検証することを特徴とする請求項１５に記載のアクセス資格認証装置。
【請求項１９】　暗号化関数が法ｎのもとでのＲＳＡ公開鍵暗号であり、アクセス資格認証の特徴情報が秘密鍵Ｄであり、秘密鍵Ｄに対応する公開鍵がＥであり、
上記第７の記憶手段に記憶される認証用素データがデータＫを法ｎのもとでＥ乗した数Ｋ’（$=K^E \mod n$）であり、
上記乱数生成手段は、生成した乱数ｒを法ｎのもとでＥ乗した数と、前記Ｋ’とを法ｎのもとで乗じた数Ｃ（$=r^E K' \mod n$）を認証用データとして前記第４の記憶手段に書き込み、
証明データ検証手段は、第６の記憶手段に記憶されている乱数ｒの法ｎのもとでの逆数を、証明データ生成装置によって第５の記憶手段に書き込まれた証明データＲに乗じた数と、前記Ｋとが法ｎのもとで合同であること（$K \mod n = r^{-1}R \mod n$）を検証することを特徴とする請求項１６に記載のアクセス資格認証装置。
【請求項２０】　暗号化関数が法ｎのもとでのＲＳＡ公開鍵暗号であり、アクセス資格認証の特徴情報が秘密鍵Ｄであり、秘密鍵Ｄに対応する公開鍵がＥであり、
上記第３の記憶手段に記憶される証明用補助情報ｔが、前記Ｄから上記第２の記憶手段に記憶されるユーザの固有情報ｅを減じ、さらに、前記ｎとｅに依存する非衝突性関数値ω（＝Ｇ（ｎ，ｅ））とｎのオイラー数φ（ｎ）との積を加えて得られるデータ（$t = D - e + \omega\varphi(n)$）であり、
上記証明データ生成手段は、前記ｔと、前記ｅと、第１の記憶手段に書き込まれた認証用データＣとから、法ｎのもとでＣのＤ乗（$C^D \mod n$）を計算することによって前記証明データを生成することを特徴とする請求項１８または１９に記載のアクセス資格認証装置。
【請求項２１】　上記証明データ生成手段が、第３の演算手段と、第４の演算手段と、第５の演算手段とからなり、
第３の演算手段は、前記法ｎのもとで前記Ｃの前記ｔ乗（$C^t \mod n$）を計算し、
第４の演算手段は、前記法ｎのもとで前記Ｃの前記ｅ乗（$C^e \mod n$）を計算し、
第５の演算手段は、前記法ｎのもとで第１および第２の演算手段の計算結果を乗じることによって、証明データＲ（$=C^t C^e \mod n$）を生成することを特徴とする請求項２０に記載のアクセス資格認証装置。

【請求項２２】　前記第２の記憶手段及び前記第４の演算手段が、内部の処理手続及びデータを外部の観測から防御する防御手段中に内蔵されることを特徴とする請求項２１に記載のアクセス資格認証装置。

【請求項２３】　暗号化関数が法ｎのもとでのＲＳＡ公開鍵暗号であり、アクセス資格認証の特徴情報が秘密鍵Ｄであり、秘密鍵Ｄに対応する公開鍵がＥであり、

上記第３の記憶手段に記憶される証明用補助情報ｔが、前記Ｄに、上記第２の記憶手段に記憶されるユーザの固有情報ｅと前記法ｎとに依存する非衝突性関数値Ｆ（ｎ，ｅ）を加えて得られるデータ（ｔ＝Ｄ＋Ｆ（ｎ，ｅ））であり、

上記証明データ生成手段は、前記ｔと、前記ｅと、前記第１の記憶手段に書き込まれた認証用データＣとから、法ｎのもとでＣのＤ乗（C^D　ｍｏｄ　ｎ）を計算することによって前記証明データを生成することを特徴とする請求項１８または１９に記載のアクセス資格認証装置。

【請求項２４】　上記証明データ生成手段が、第３の演算手段と、第４の演算手段と、第５の演算手段とからなり、

第３の演算手段は、前記法ｎのもとで前記Ｃの前記ｔ乗（C^t　ｍｏｄ　ｎ）を計算し、

第４の演算手段は、前記法ｎのもとで前記Ｃの前記Ｆ（ｎ，ｅ）乗（$C^{F(n,e)}$ｍｏｄ　ｎ）を計算し、

第５の演算手段は、前記法ｎのもとで、第３の演算手段の計算結果と、第４の演算手段の計算結果の逆数とを乗じることによって、証明データＲ（$=C^tC^{-F(n,e)}$　ｍｏｄ　ｎ）を生成することを特徴とする請求項２３に記載のアクセス資格認証装置。

【請求項２５】　前記第２の記憶手段及び前記第４の演算手段が、内部の処理手続及びデータを外部の観測から防御する防御手段中に内蔵されることを特徴とする請求項２４に記載のアクセス資格認証装置。

【請求項２６】　暗号化関数が法ｐのもとでのＰｏｈｌｉｇ－Ｈｅｌｌｍａｎ非対称鍵暗号であり、アクセス資格認証の特徴情報が一方の鍵Ｄであり、鍵Ｄに対応する他方の鍵がＥであり（ＤＥ　ｍｏｄ　ｐ－１　＝　１）、

証明データ検証手段は、第５の記憶手段に書き込まれた証明データＲをＥ乗した結果と、第４の記憶手段に記憶されている認証用データＣとが法ｐのもとで合同であること（R^E　ｍｏｄ　ｐ　＝　Ｃ　ｍｏｄ　ｐ）を検証することを特徴とする請求項１５に記載のアクセス資格認証装置。

【請求項２７】　暗号化関数が法ｐのもとでのＰｏｈｌｉｇ－Ｈｅｌｌｍａｎ非対称鍵暗号であり、アクセス資格認証の特徴情報が一方の鍵Ｄであり、鍵Ｄに対応する他方の鍵がＥであり（ＤＥ　ｍｏｄ　ｐ－１　＝　１）、

上記第７の記憶手段に記憶される認証用素データがデータＫを法ｐのもとでＥ乗した数Ｋ’（$=K^E$　ｍｏｄ　ｐ）であり、

上記乱数生成手段は、生成した乱数ｒを法ｐのもとでＥ乗した数と、前記Ｋ’とを法ｐのもとで乗じた数Ｃ（$=r^EK'$　ｍｏｄ　ｐ）を認証用データとして前記第４の記憶手段に書き込み、

証明データ検証手段は、第６の記憶手段に記憶されている乱数ｒの法ｐのもとでの逆数を、証明データ生成装置によって第５の記憶手段に書き込まれた証明データＲに乗じた数と、前記Ｋとが法ｐのもとで合同であること（Ｋ　ｍｏｄ　ｐ＝r^{-1}Ｒ　ｍｏｄ　ｐ）を検証することを特徴とする請求項１６に記載のアクセス資格認証装置。

【請求項２８】　暗号化関数が法ｐのもとでのＰｏｈｌｉｇ－Ｈｅｌｌｍａｎ非対称鍵暗号であり、アクセス資格認証の特徴情報が一方の鍵Ｄであり、鍵Ｄに対応する他方の鍵がＥであり（ＤＥ　ｍｏｄ　ｐ－１　＝　１）、

上記第３の記憶手段に記憶される証明用補助情報ｔが、前記Ｄに、上記第２の記憶手段に記憶されるユーザ固有情報ｅと前記ｐとに依存する非衝突性関数値Ｆ（ｐ，ｅ）を加えて得られるデータ（ｔ＝Ｄ＋Ｆ（ｐ，ｅ））であり、

上記証明データ生成手段は、前記ｔと、前記ｅと、第１の記憶手段に書き込まれた認証用データＣとから、法ｐのもとでＣのＤ乗（C^D　ｍｏｄ　ｐ）を計算することによって前記証明データを生成することを特徴とする請求項２６または２７に記載のアクセス資格認証装置。

【請求項２９】　上記証明データ生成手段が、第３の演算手段と、第４の演算手段と、第５の演算手段とからなり、

第３の演算手段は、前記法ｐのもとで前記Ｃの前記ｔ乗（C^t　ｍｏｄ　ｐ）を計算し、

第４の演算手段は、前記法ｐのもとで、前記Ｆ（ｐ，ｅ）を指数として、前記Ｃのべき乗（$C^{F(p,e)}$　ｍｏｄ　ｐ）を計算し、

第５の演算手段は、前記法ｐのもとで、第３の演算手段の計算結果と、第４の演算手段の計算結果の逆数とを乗じることによって、証明データＲ（$=C^tC^{-F(p,e)}$　ｍｏｄ　ｐ）を生成することを特徴とする請求項２８に記載のアクセス資格認証装置。

【請求項３０】　前記第２の記憶手段及び前記第４の演算手段が、内部の計算手順及びデータを外部の観測から防御する防御手段中に内蔵されることを特徴とする請求項２９に記載のアクセス資格認証装置。

【請求項３１】　暗号化関数が法ｐ、生成元ａのもとでのＥｌＧａｍａｌ公開鍵暗号であり、アクセス資格認証の特徴情報が一方の鍵Ｘであり、鍵Ｘに対応する公開鍵がＹであり（Ｙ　＝　a^X　ｍｏｄ　ｐ）、

ｕが上記ａを法ｐのもとで適当な乱数ｚを指数としてべき乗した数であり（ｕ＝a^z ｍｏｄ ｐ）、
Ｋ’が、上記Ｙを法ｐのもとで上記乱数ｚを指数としてべき乗した数と、データＫとの積であるとき（Ｋ’＝Y^zK ｍｏｄ ｐ）、
上記第７の記憶手段に認証用素データとしてｕ及びＫ’の組が記憶され、
上記乱数生成手段は、上記ｕと、生成した乱数ｒを前記Ｋ’に法ｐのもとで乗じた数Ｃ（＝ｒＫ’ ｍｏｄ ｐ）とを認証用データとして前記第４の記憶手段に書き込み、
証明データ検証手段は、第６の記憶手段に記憶されている乱数ｒの法ｐのもとでの逆数を、証明データ生成装置によって第５の記憶手段に書き込まれた証明データＲに乗じた数と、前記Ｋとが法ｐのもとで合同であること（Ｋ ｍｏｄ ｐ＝r^{-1}Ｒ ｍｏｄ ｐ）を検証することを特徴とする請求項１６に記載のアクセス資格認証装置。

【請求項３２】　暗号化関数が法ｐ、生成元ａのもとでのＥｌＧａｍａｌ公開鍵暗号であり、アクセス資格認証の特徴情報が一方の鍵Ｘであり、鍵Ｘに対応する公開鍵がＹであり（Ｙ ＝ a^X ｍｏｄ ｐ）、
上記第３の記憶手段に記憶される証明用補助情報ｔが、前記Ｘに、上記第２の記憶手段に記憶されるユーザ固有情報ｅと前記ｐとに依存する非衝突性関数値Ｆ（ｐ，ｅ）を加えて得られるデータ（ｔ＝Ｘ＋Ｆ（ｐ，ｅ））であり、
上記証明データ生成手段は、前記ｔと、前記ｅと、第１の記憶手段に書き込まれた認証用データｕ及びＣから、法ｐのもとで、Ｃを上記ｕのＸ乗で割った数（Cu^{-X} ｍｏｄ ｐ）を計算することによって上記証明データを生成することを特徴とする請求項３１に記載のアクセス資格認証装置。

【請求項３３】　上記証明データ生成手段が、第３の演算手段と、第４の演算手段と、第５の演算手段とからなり、
第３の演算手段は、前記法ｐのもとで前記ｕの前記ｔ乗（u^t ｍｏｄ ｐ）を計算し、
第４の演算手段は、前記法ｐのもとで前記ｕの前記Ｆ（ｐ，ｅ）乗（$u^{F(p,e)}$ｍｏｄ ｎ）を計算し、
第５の演算手段は、前記法ｐのもとで、上記Ｃを第３の演算手段の計算結果で割り、さらに、第４の演算手段の計算結果を乗じることによって、証明データＲ（＝$Cu^{-t}u^{F(p,e)}$ ｍｏｄ ｐ）を生成することを特徴とする請求項３２に記載のアクセス資格認証装置。

【請求項３４】　前記第２の記憶手段及び前記第４の演算手段が、内部の計算手順及びデータを外部の観測から防御する防御手段中に内蔵されることを特徴とする請求項３３に記載のアクセス資格認証装置。

【請求項３５】　署名関数が法ｐ、生成元ａのもとでのＥｌＧａｍａｌ署名であり、アクセス資格認証の特徴情報が一方の鍵Ｘであり、鍵Ｘに対応する公開鍵がＹであり（Ｙ ＝ a^X ｍｏｄ ｐ）、
証明データ検証手段は、第５の記憶手段に書き込まれた証明データＲ及びＳに対して、法ｐのもとで、上記ａを第４の記憶手段に記憶されている認証用データＣを指数としてべき乗した値と、上記Ｙを Ｒ乗した値とＲをＳ乗した値との積とが法ｐのもとで合同であること（a^C ｍｏｄ ｐ ＝ Y^RR^S ｍｏｄ ｐ）を検証することを特徴とする請求項１７に記載のアクセス資格認証装置。

【請求項３６】　署名関数が法ｐ、生成元ａのもとでのＥｌＧａｍａｌ署名であり、アクセス資格認証の特徴情報が一方の鍵Ｘであり、鍵Ｘに対応する公開鍵がＹであり（Ｙ ＝ a^X ｍｏｄ ｐ）、
上記第３の記憶手段に記憶される証明用補助情報ｔが、前記Ｘに、上記第２の記憶手段に記憶されるユーザ固有情報ｅと前記ｐとに依存する非衝突性関数値Ｆ（ｐ，ｅ）を加えて得られるデータ（ｔ＝Ｘ＋Ｆ（ｐ，ｅ））であり、
上記証明データ生成手段は、証明データＲ及びＳを生成するに当たり、適当な乱数ｋを生成し、法ｐのもとでの上記ａのｋ乗をＲ（＝a^k ｍｏｄ ｐ）とし、前記ｔと、前記ｅと、第１の記憶手段に書き込まれた認証用データＣから、法ｐ－１のもとで、ＣからＸとｒの積を引いた数にｋの逆数を乗じることによって、Ｓ（＝（Ｃ－ＲＸ）k^{-1} ｍｏｄ ｐ－１）を計算することを特徴とする請求項３５に記載のアクセス資格認証装置。

【請求項３７】　第２の記憶手段及び証明データ生成手段が、内部の計算手順及びデータを外部の観測から防御する防御手段中に内蔵されることを特徴とする請求項３６に記載のアクセス資格認証装置。

【請求項３８】　上記ユーザの固有情報が暗号関数の復号鍵であり、証明用補助情報がアクセス資格認証のための特徴情報を前記復号鍵に対応する暗号化鍵によって暗号化したものであり、第１の演算手段は上記ユーザの固有情報である復号鍵を用いて、証明用補助情報を復号することにより、アクセス資格認証のための特徴情報を算出することを特徴とする請求項４に記載のアクセス資格認証装置。

【請求項３９】　上記暗号関数が非対称鍵暗号関数であり、ユーザの固有情報が一方の鍵であることを特徴とする請求項３８に記載のアクセス資格認証装置。

【請求項４０】　上記暗号関数が公開鍵暗号関数であり、ユーザの固有情報が秘密鍵であることを特徴とする請求項３９に記載のアクセス資格認証装置。

【請求項４１】　上記暗号関数が対称鍵暗号関数であり、ユーザの固有情報が共通秘密鍵であることを特徴とする請求項３８に記載のアクセス資格認証装置。

【請求項４２】　上記証明データ検証手段は、暗号化さ

れたデータである上記認証用データあるいは上記認証用素データに対応する平文データを記憶する第8の記憶手段と、比較手段とを有し、
上記比較手段は、上記証明データ生成手段が生成した上記証明データ或は証明データから乱数効果を除去した結果と、第8の記憶手段に記憶されている平文データを比較し、両者が一致した場合に限り、上記証明データが正当であると判断することを特徴とする請求項8または16に記載のアクセス資格認証装置。
【請求項43】　上記証明データ検証手段は、暗号化されたデータである上記認証用データあるいは上記認証用素データに対応する平文データに所定の一方向関数を施した結果を記憶する第9の記憶手段と、上記一方向関数を実行する第6の演算手段と、比較手段とを有し、
第6の演算手段は、上記証明データ生成手段が生成した上記証明データに、必要ならば乱数効果を取り除いたのち、一方向関数を施し、
上記比較手段は、第6の演算手段による計算結果と、第9の記憶手段に記憶されているデータを比較し、両者が一致した場合に限り、上記証明データが正当であると判断することを特徴とする請求項8または16に記載のアクセス資格認証装置。
【請求項44】　上記証明データ検証手段は、プログラム実行手段を含み、上記認証用データあるいは上記認証用素データは、プログラムを暗号化して得られるデータであり、
上記証明データ検証手段が、証明データ生成手段が生成した上記証明データを、必要ならば乱数効果を取り除いたのち、プログラムとしてプログラム実行手段に引き渡すことにより、
証明データ生成手段が、暗号化されたプログラムである上記認証用データあるいは認証用素データを正しく復号した場合、即ち、暗号化されたプログラムが正しく復号された場合に限り、プログラム実行手段が正しい動作を行うことを特徴とする請求項8または16に記載のアクセス資格認証装置。
【請求項45】　上記証明データ検証手段は、プログラム実行手段と、プログラム記憶手段と、プログラム復号手段とを含み、
プログラム記憶手段に記憶されているプログラムは、その一部あるいは全部が暗号化されたものであり、
上記認証用データあるいは上記認証用素データは、前記暗号化されたプログラムを復号するための復号鍵を別途暗号化して得られるデータであり、
上記証明データ検証手段は、証明データ生成手段が生成した上記証明データをプログラム復号手段に引き渡し、
プログラム復号手段は、前記証明データ生成手段が生成した証明データを、必要ならば乱数効果を取り除いたのち、復号鍵として用いることにより、プログラム記憶手段に記憶されたプログラムの必要な部分を復号し、
プログラム実行手段が復号されたプログラムを実行することにより、
証明データ生成手段が上記認証用データあるいは認証用素データを正しく復号した場合、即ち、暗号化されたプログラムを復号するために復号鍵が正しく復号された場合に限り、プログラム実行手段が正しい動作を行うことを特徴とする請求項8または16に記載のアクセス資格認証装置。
【請求項46】　上記証明データ生成装置および上記証明データ認証装置が同一の筐体内に設けられ、上記証明データ生成装置および上記証明データ認証装置が、当該筐体の外部の通信媒体を解さずに通信を行う請求項14に記載のアクセス資格認証装置。
【請求項47】　ユーザのアクセス資格を証明するために認証用データから生成された証明データの正当性を検証することにより上記ユーザのアクセス資格を認証するアクセス資格認証方法において、
上記認証用データを記憶するステップとユーザの固有情報を記憶するステップと、
上記ユーザの固有情報と、アクセス資格認証の特徴情報とに対し、所定の計算を実行した実行結果である証明用補助情報を記憶するステップと、
上記認証用データと、上記ユーザの固有情報と、上記証明用補助情報とに所定の計算を施して証明データを生成するステップと、
上記証明データ生成手段によって生成された証明データが上記アクセス資格認証の特徴情報に基づいて生成されていることを検証するステップとを有することを特徴とするアクセス資格認証方法。
【請求項48】　ユーザのアクセス資格を証明するために認証用データから生成された証明データの正当性を検証することにより上記ユーザのアクセス資格を認証するために、コンピュータで用いられるアクセス資格認証用プログラム製品において、
上記認証用データを記憶するステップと、
ユーザの固有情報を記憶するステップと、
上記ユーザの固有情報と、アクセス資格認証の特徴情報とに対し、所定の計算を実行した実行結果である証明用補助情報を記憶するステップと、
上記認証用データと、上記ユーザの固有情報と、上記証明用補助情報とに所定の計算を施して証明データを生成するステップと、
上記証明データ生成手段によって生成された証明データが上記アクセス資格認証の特徴情報に基づいて生成されていることを検証するステップとを上記コンピュータに実行させるのに用いることを特徴とするアクセス資格認証用プログラム製品。
【請求項49】　ユーザのアクセス資格を認証するためにその正当性を検証される証明データを、認証用データから生成するために、コンピュータで用いられる証明デ

ータ生成用プログラム製品において、
上記認証用データを記憶するステップと、
ユーザの固有情報を記憶するステップと、
上記ユーザの固有情報と、アクセス資格認証の特徴情報とに対し、所定の計算を実行した実行結果である証明用補助情報を記憶するステップと、
上記認証用データと、上記ユーザの固有情報と、上記証明用補助情報とに所定の計算を施して証明データを生成するステップとを上記コンピュータに実行させるのに用いられることを特徴とする証明データ生成用プログラム製品。
【請求項５０】　ユーザのアクセス資格を証明するために生成された証明データの正当性を検証することにより上記ユーザのアクセス資格を認証し、上記資格の認証に基づいてプログラムの実行を制御するプログラム実行制御装置において、
認証用データを記憶する第１の記憶手段と、
ユーザの固有情報を記憶する第２の記憶手段と、
上記ユーザの固有情報と、アクセス資格認証の特徴情報とに対し、所定の計算を実行した実行結果である証明用補助情報を記憶する第３の記憶手段と、
上記第２の記憶手段に記憶されている上記ユーザの固有情報と、上記第３の記憶手段に記憶されている上記証明用補助情報とを利用して、上記認証用データから上記証明データを生成する証明データ生成手段と、
上記証明データ生成手段から生成された証明データの正当性を検証する手段と、
上記証明データの正当性が検証されたときにプログラムの実行を継続する手段とを有することを特徴とするプログラム実行制御装置。
【請求項５１】　所定の情報処理資源へのユーザのアクセス資格を証明するために生成された証明データの正当性を検証することにより上記ユーザのアクセス資格を認証して上記所定の情報処理資源へのアクセスを許容する情報処理装置において、
認証用データを記憶する第１の記憶手段と、
ユーザの固有情報を記憶する第２の記憶手段と、
上記ユーザの固有情報と、アクセス資格認証の特徴情報とに対し、所定の計算を実行した実行結果である証明用補助情報を記憶する第３の記憶手段と、
上記第２の記憶手段に記憶されている上記ユーザの固有情報と、上記第３の記憶手段に記憶されている上記証明用補助情報とを利用して、上記認証用データから上記証明データを生成する証明データ生成手段と、
上記証明データ生成手段から生成された証明データの正当性を検証する手段と、
上記正当性の検証に基づいて上記所定の情報処理資源へのアクセスを許可する手段とを有することを特徴とする情報処理装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】この発明はユーザのアクセス資格を認証するアクセス資格認証装置および方法に関する。
【０００２】
【従来の技術】
［関連技術］この発明と同分野に属する先行技術としてプログラムの実行制御技術が知られている。プログラム実行制御技術は、
１．アプリケーションプログラム中に、ユーザのアクセス資格認証のためのルーチンを埋め込み、
２．該ルーチンはアプリケーションの実行を試みているユーザが正規の認証用の鍵を保有していることを検査し、
３．上記認証用の鍵の存在が確認された場合に限りプログラムを続行し、それ以外の場合にはプログラムの実行を停止する
技術である。当技術を利用することにより、認証鍵を保有する正規のユーザにのみアプリケーションプログラムの実行を可能ならしめることが出来る。当技術はソフトウェア頒布事業において実用化されており、製品として、例えばＲａｉｎｂｏｗ　Ｔｅｃｈｎｏｌｏｇｉｅｓ，Ｉｎｃ．社のＳｅｎｔｉｎｅｌ　ＳｕｐｅｒＰｒｏ（商標）や、Ａｌａｄｄｉｎ　Ｋｎｏｗｌｅｄｇｅ　ＳｙｓｔｅｍｓｓＬｔｄ．社のＨＡＳＰ（商標）等がある。
【０００３】以下にプログラム実行制御技術についてより詳細に説明する。
１．ソフトウェアの実行を行なうユーザはユーザ固有情報として認証鍵を保有する。認証鍵は暗号化のための鍵であり、ソフトウェアの利用を許可する者、例えばソフトウェアベンダがユーザに配布する。認証鍵は複製を防ぐためにハードウェア中のメモリ等に厳重に封入され、郵便等の物理的手段を用いてユーザに配送される。
２．ユーザは認証鍵を内蔵したハードウェアを指定された方法で所有のパソコン・ワークステーションに装着する。ハードウェアは、例えばプリンタポートに装着される。
３．ユーザがアプリケーションプログラムを起動し、プログラムの実行が上記アクセス資格認証ルーチンに及ぶと、プログラムはユーザの認証鍵を内蔵したハードウェアと通信する。通信の結果に基づいてプログラムは認証鍵を識別し、正しい認証鍵の存在が確認されると次のステップへ実行を移す。通信が失敗し認証鍵の存在が確認できない場合は、プログラムは自らを停止し以降の実行ができないようにする。
【０００４】アクセス資格認証ルーチンによる認証鍵の識別は、例えば、次のようなプロトコルに従って行なわれる。
１．アクセス資格認証ルーチンは適当な数を生成し鍵内

蔵ハードウェアに送信する。
２．鍵内蔵ハードウェアは内蔵する認証鍵を用いて送られた数を暗号化し、上記アクセス資格認証ルーチンに返信する。
３．認証ルーチンは、返信された数が予め予想された数、即ちハードウェアに送信した数を正しい認証鍵で暗号化して得られる数であるか否かを判定する。
４．返信された数が予想された数と一致する場合にはプログラムの実行を続行し、一致しない場合には停止する。
【０００５】この際、アプリケーションプログラムと認証鍵内蔵ハードウェア間の通信は、たとえ同じアプリケーションプログラム中の同じ箇所において同じハードウェアとの間で交換されるものであろうとも、実行のたびに異ならなければならない。さもなければ、正常な実行過程における通信内容を一度記録し、以後プログラムを実行する度に記録した通りにアプリケーションプログラムへの返信を行なうことにより、正しい認証鍵を保有しないユーザでもプログラムを実行することが可能となってしまう。このような通信内容の再現によるアプリケーションプログラムの不正実行をリプレイアタック（ｒｅｐｌａｙ　ａｔｔａｃｋ）と呼ぶ。
【０００６】リプレイアタックを防ぐために、通常、鍵内蔵ハードウェアに送られる数は通信の度に新たに生成される乱数を用いる。
【０００７】［従来技術の問題点］従来技術の問題点は、アプリケーションプログラムを作成する際に、プログラム作成者がユーザが持つ認証鍵を予め想定した上で、該認証鍵に基づいてプログラムの保護処理を行なわなければならないという性質に由来する。つまり、プログラム作成者は、鍵内蔵ハードウェアからの正しい返信をプログラム作成時に予測して、正しい返信を受けた場合にのみプログラムが正常に実行されるようにプログラムの作成を行なわなければならない。
【０００８】上記特徴を有する従来技術の利用形態は基本的に二通りとなるが、いずれの場合も以下に述べる問題を有する。
【０００９】１．第一の方法ではユーザの認証鍵をユーザ毎に異なるように用意する。即ち、ユーザ甲には認証鍵甲、ユーザ乙には認証鍵乙というように、ユーザ毎に異なる認証鍵を一つずつ用意する。
【００１０】この場合、プログラム作成者は、プログラム中の認証ルーチンをユーザ毎に適切に変えてプログラムを作成する必要がある。つまり、ユーザ毎に認証鍵が異なるので、プログラム中の認証ルーチンは該プログラムを利用するユーザ固有の認証鍵を識別するように作成されなければならず、プログラム作成者は利用ユーザの数だけ異なるプログラムを作成する必要がある。
【００１１】対象となるユーザが多数の場合、プログラムをユーザ毎に個別化する作業はプログラム作成者にとって耐えがたい労力を要求し、管理しなければならないユーザ認証鍵のリストも膨大なものとなる。
【００１２】２．第二の方法では、プログラム作成者はアプリケーション毎にそれぞれ異なる認証鍵を用意する。即ち、アプリケーション甲には認証鍵甲、アプリケーション乙には認証鍵乙というように、アプリケーション毎に異なる認証鍵を一つずつ用意し、固有の認証鍵を識別するように各アプリケーションプログラムを作成する。
【００１３】この方法では、第一の方法の場合のようにユーザ毎にプログラムを個別的に作成する必要は無くなるが、逆に、ユーザは利用するアプリケーションの数だけ認証鍵を保持しなければならないこととなる。
【００１４】この制約はプログラム作成者およびユーザそれぞれに以下のような問題を惹起する。
【００１５】前述のように、認証鍵はハードウェアに厳重に封入した状態でユーザに配布する必要がある。従って、プログラム自身はネットワークを介して簡便に配布することができるのに対し、認証鍵を内蔵するハードウェアの配布は郵便等の物理手段に頼らざるを得ない。プログラム作成者はユーザからアプリケーションの使用許諾以来を受ける度に、このアプリケーションに対応する認証鍵が封入されたハードウェアを郵送する必要があり、コスト、時間、梱包の手間いずれをとっても、プログラム作成者とって大きな負担となる。
【００１６】プログラム作成者は、ユーザの要求に応えるべく、アプリケーション毎に異なるハードウェアを一定個数ストックしておかなければならず、在庫管理のコストを必要とする。
【００１７】また、ユーザは利用するアプリケーションを変更する度にハードウェアを交換しなければならないという煩雑さに甘んじなければならない。
【００１８】ユーザがあるアプリケーションを使いたいとしても、認証鍵が封入されたハードウェアが郵送されるまで待たねばならず即座に利用できないという不便もある。
【００１９】この負担を軽減するため、ハードウェア中に複数の認証鍵を予め封入しておき、新しいアプリケーションの利用をユーザに許可する度に、ハードウェア中の未使用の認証鍵を利用可能とするためのパスワードをユーザに教えるといった方法が用いられる。しかしながら、この方法を用いたとしても、上記の問題点は原理的に解決されないことは明らかである。実際、商品化に際しては、ハードウェアは連接して複数結合することが可能となるように設計され、上記問題点に起因する不便さを緩和するようにしてある。
【００２０】このように、上記二つのいずれの方法をとったとしても、プログラム作成者およびユーザの利便に問題が存在する。
【００２１】なお、実行制御の外的な特質を考えると、

メールのプライバシー保護やファイルや計算機資源のアクセス制御にも適用可能であると想像できる。しかしながら、従来技術をこれらの分野に適用しようとしても、上記の問題点により不可能である。

【００２２】

【発明が解決しようとする課題】この発明は、以上の事情を考慮してなされたものであり、多数の認証鍵等の固有情報を取り扱うことから派生する不具合から、ユーザ側およびアプリケーション作成者等のプロテクト側の双方を解消し、もってプログラムの実行制御、メールのプライバシ保護、ファイルや計算機資源のアクセス制御等を行う際にユーザのアクセス資格を簡易に認証することができるようにしたアクセス資格認証技術を提供することを目的としている。

【００２３】

【課題を解決する手段】この発明の第１の側面によれば、上述の目的を達成するために、ユーザのアクセス資格を証明するために生成された証明データの正当性を検証することにより上記ユーザのアクセス資格を認証するアクセス資格認証装置に、認証用データを記憶する第１の記憶手段と、ユーザの固有情報を記憶する第２の記憶手段と、上記ユーザの固有情報と、アクセス資格認証の特徴情報とに対し、所定の計算を実行した実行結果である証明用補助情報を記憶する第３の記憶手段と、上記第１の記憶手段に保持されている認証用データと、上記第２の記憶手段に記憶されている上記ユーザの固有情報と、上記第３の記憶手段に記憶されている上記証明用補助情報とに所定の計算を施して証明データを生成する証明データ生成手段と、上記証明データ生成手段によって生成された証明データが上記アクセス資格認証の特徴情報に基づいて生成されていることを検証する証明データ検証手段とを設けるようにしている。

【００２４】この構成によれば、証明用補助データ（アクセスチケット）を導入することにより、プロテクト側で付与されるアクセス資格認証用の特徴情報とユーザ側に付与されるユーザ固有情報とを独立させることができる。ユーザはあらかじめユーザ固有情報を所持し、プログラム作成者等のプロテクト者はユーザが所持するユーザ固有情報とは独立にアクセス資格認証の特徴情報を用意し、アクセスチケットをユーザの固有情報とアプリケーションプログラムの作成等に使用したアクセス資格認証の特徴情報とに応じて作成し、配布することにより、実行制御等のユーザのアクセス資格の認証を行なうことができる。このようにして、ユーザもプロテクト側も同一の情報を用いて認証を行う場合に生じる煩雑さを回避できる。

【００２５】また、この構成においては、少なくとも、上記第２の記憶手段と、上記証明データ生成手段とが、内部のデータ及び処理手続を外部から観測することを困難ならしめる防御手段中に保持されるようにしてもよい。また、少なくとも、上記第２の記憶手段と、上記証明データ生成手段とが、ＩＣカードなどの携帯可能な小型演算装置として構成されるようにしてもよい。

【００２６】また、上記証明データ生成手段が、第１の演算手段と、第２の演算手段とから構成され、第１の演算手段は、上記第２の記憶手段に記憶されているユーザの固有情報と、上記第３の記憶手段に記憶されている証明用補助情報とに所定の計算を施し、その結果として上記アクセス資格認証の特徴情報を算出し、第２の演算手段は、上記第１の記憶手段に記憶されている認証用データと、第１の演算手段によって算出されたアクセス資格認証の特徴情報とに所定の計算を施し、その結果として上記証明データを生成するようにすることもできる。

【００２７】また、上記証明データ生成手段が、第３の演算手段と、第４の演算手段と、第５の演算手段とから構成され、第３の演算手段は、上記第１の記憶手段に記憶されている認証用データと、上記第３の記憶手段に記憶されている証明用補助情報とに所定の計算を施し、第４の演算手段は、上記第１の記憶手段に記憶されている認証用データと、第２の記憶手段に記憶されているユーザの固有情報とに所定の計算を施し、第５の演算手段が、上記第３の演算手段による計算結果と、上記第４の演算手段による計算結果とに所定の計算を施し、その結果として上記証明データを生成するようにすることもできる。この場合においても、少なくとも、上記第２の記憶手段と、上記第４の演算手段とが、内部のデータ及び処理手続を外部から観測することを困難ならしめる防御手段中に保持されるようにしてもよい。また、少なくとも、上記第２の記憶手段と、上記第４の演算手段とが、ＩＣカードなどの携帯可能な小型演算装置として構成されるようにすることもできる。この構成では、防御手段中に保持する手段を小規模にすることができ、特にＩＣチップ等を用いた小型の構成が要求される実施態様において有効である。

【００２８】また、上記アクセス資格認証の特徴情報が暗号関数における復号鍵であり、上記認証用データが適当なデータを前記復号鍵に対応する暗号化鍵を用いて暗号化したものであり、上記証明データ検証手段は、上記証明データ生成手段が生成する上記証明データが認証用データを正しく復号したものであることを検証するようにしてもよい。

【００２９】また、上記アクセス資格認証の特徴情報が暗号関数における暗号化鍵であり、上記証明データ生成手段が生成する上記証明データが上記認証用データを前記暗号化鍵を用いて正しく暗号化したものであることを検証するようにしてもよい。

【００３０】また、上記アクセス資格認証の特徴情報がデジタル署名関数における署名鍵であり、上記証明データ生成手段が生成する上記証明データが、上記認証用データに対して、前記署名鍵を用いて正しく生成されたデ

ジタル署名であることを検証するようにしてもよい。

【００３１】また、暗号化関数が非対称鍵暗号関数であり、アクセス資格認証の特徴情報が鍵の一方であってもよい。

【００３２】また、暗号化関数が公開鍵暗号関数であり、アクセス資格認証の特徴情報が秘密鍵であってもよい。

【００３３】また、暗号化関数が対称鍵暗号関数であり、アクセス資格認証の特徴情報が共通秘密鍵であってもよい。

【００３４】また、上記第１の記憶手段と、上記第２の記憶手段と、上記第３の記憶手段と、上記証明データ生成手段とから構成される証明データ生成装置と、上記証明データ検証手段に加え、認証用データを記憶する第４の記憶手段と、証明データを記憶する第５の記憶手段を備えた証明データ検証装置とが、互いに通信することによりユーザのアクセス資格を認証するアクセス資格認証装置において、証明データ検証装置は、第４の記憶手段に記憶されている認証用データを証明データ生成装置の第１の記憶手段に書き出し、証明データ生成装置は、証明データ生成手段によって第１の記憶手段に書き込まれた上記認証用データをもとに生成した証明データを、証明データ検証装置中の第５の記憶手段に書き出し、証明データ検証装置は第５の記憶手段に書き込まれた上記証明データを用いてユーザのアクセス資格を認証するようにすることもできる。

【００３５】また、上記アクセス資格認証の特徴情報が暗号化関数の暗号化鍵であり、証明データ検証装置が乱数生成手段を備え、乱数生成手段は生成した乱数を認証用データとして第４の記憶手段に書き込み、証明データ検証手段は、証明データ生成装置によって第５の記憶手段に書き込まれた証明データが前記乱数である認証用データをアクセス資格認証の特徴情報である暗号化鍵で暗号化したものであることを検証するようにしてもよい。

【００３６】また、アクセス資格認証の特徴情報が暗号化関数の復号鍵であり、証明データ検証装置が乱数生成手段と、生成した乱数を記憶する第６の記憶手段と、認証用素データを記憶する第７の記憶手段とを備え、乱数生成手段は生成した乱数を第６の記憶手段に書き込むと共に、第７の記憶手段に記憶されている認証用素データに前記乱数を用いた乱数効果を施した後、認証用データとして第４の記憶手段に書き込み、証明データ検証手段は、第６の記憶手段に記憶されている乱数による乱数効果を、上記証明データ生成装置によって第５の記憶手段に書き込まれた証明データから除去した結果が、アクセス資格認証の特徴情報である復号鍵で第７の記憶手段に記憶されている認証用素データを復号したものであることを検証するようにしてもよい。

【００３７】また、上記アクセス資格認証の特徴情報がデジタル署名関数の署名鍵であり、証明データ検証装置が乱数生成手段を備え、乱数生成手段は生成した乱数を認証用データとして第４の記憶手段に書き込み、証明データ検証手段は、証明データ生成装置によって第５の記憶手段に書き込まれた証明データが、前記乱数である認証用データに対する、アクセス資格認証の特徴情報である署名鍵によるデジタル署名であることを検証するようにしてもよい。

【００３８】また、暗号化関数が法ｎのもとでのＲＳＡ公開鍵暗号であり、アクセス資格認証の特徴情報が秘密鍵Ｄであり、秘密鍵Ｄに対応する公開鍵がＥであり、証明データ検証手段は、第５の記憶手段に書き込まれた証明データＲをＥ乗した結果と、第４の記憶手段に記憶されている認証用データＣとが、法ｎのもとで合同であること（$R^E \mod n = C \mod n$）を検証するようにしてもよい。

【００３９】また、暗号化関数が法ｎのもとでのＲＳＡ公開鍵暗号であり、アクセス資格認証の特徴情報が秘密鍵Ｄであり、秘密鍵Ｄに対応する公開鍵がＥであり、上記第７の記憶手段に記憶される認証用素データがデータＫを法ｎのもとでＥ乗した数Ｋ’（$=K^E \mod n$）であり、上記乱数生成手段は、生成した乱数ｒを法ｎのもとでＥ乗した数と、前記Ｋ’とを法ｎのもとで乗じた数Ｃ（$=r^E K' \mod n$）を認証用データとして前記第４の記憶手段に書き込み、証明データ検証手段は、第６の記憶手段に記憶されている乱数ｒの法ｎのもとでの逆数を、証明データ生成装置によって第５の記憶手段に書き込まれた証明データＲに乗じた数と、前記Ｋとが法ｎのもとで合同であること（$K \mod n = r^{-1}R \mod n$）を検証するようにしてもよい。

【００４０】また、暗号化関数が法ｎのもとでのＲＳＡ公開鍵暗号であり、アクセス資格認証の特徴情報が秘密鍵Ｄであり、秘密鍵Ｄに対応する公開鍵がＥであり、上記第３の記憶手段に記憶される証明用補助情報ｔが、前記Ｄから上記第２の記憶手段に記憶されるユーザの固有情報ｅを減じ、さらに、前記ｎとｅに依存する非衝突性関数値ω（＝Ｇ（ｎ，ｅ））とｎのオイラー数φ（ｎ）との積を加えて得られるデータ（$t=D-e+\omega\phi(n)$）であり、上記証明データ生成手段は、前記ｔと、前記ｅと、第１の記憶手段に書き込まれた認証用データＣとから、法ｎのもとでＣのＤ乗（$C^D \mod n$）を計算することによって前記証明データを生成するようにしてもよい。

【００４１】また、上記証明データ生成手段が、第３の演算手段と、第４の演算手段と、第５の演算手段とからなり、第３の演算手段は、前記法ｎのもとで前記Ｃの前記ｔ乗（$C^t \mod n$）を計算し、第４の演算手段は、前記法ｎのもとで前記Ｃの前記ｅ乗（$C^e \mod n$）を計算し、第５の演算手段は、前記法ｎのもとで第１および第２の演算手段の計算結果を乗じることによって、証明データＲ（$=C^t C^e \mod n$）を生成す

るようにしてもよい。この場合にも、前記第２の記憶手段及び前記第４の演算手段が、内部の処理手続及びデータを外部の観測から防御する防御手段中に内蔵されるようにしてもよい。

【００４２】また、暗号化関数が法ｎのもとでのＲＳＡ公開鍵暗号であり、アクセス資格認証の特徴情報が秘密鍵Ｄであり、秘密鍵Ｄに対応する公開鍵がＥであり、上記第３の記憶手段に記憶される証明用補助情報ｔが、前記Ｄに、上記第２の記憶手段に記憶されるユーザの固有情報ｅと前記法ｎとに依存する非衝突性関数値Ｆ（ｎ，ｅ）を加えて得られるデータ（ｔ＝Ｄ＋Ｆ（ｎ，ｅ））であり、上記証明データ生成手段は、前記ｔと、前記ｅと、前記第１の記憶手段に書き込まれた認証用データＣとから、法ｎのもとでＣのＤ乗（C^D ｍｏｄ ｎ）を計算することによって前記証明データを生成するようにしてもよい。

【００４３】また、上記証明データ生成手段が、第３の演算手段と、第４の演算手段と、第５の演算手段とからなり、第３の演算手段は、前記法ｎのもとで前記Ｃの前記ｔ乗（C^t ｍｏｄ ｎ）を計算し、第４の演算手段は、前記法ｎのもとで前記Ｃの前記Ｆ（ｎ，ｅ）乗（$C^{F(n,e)}$ ｍｏｄ ｎ）を計算し、第５の演算手段は、前記法ｎのもとで、第３の演算手段の計算結果と、第４の演算手段の計算結果の逆数とを乗じることによって、証明データＲ（$=C^tC^{-F(n,e)}$ ｍｏｄ ｎ）を生成するようにしてもよい。

【００４４】また、前記第２の記憶手段及び前記第４の演算手段が、内部の処理手続及びデータを外部の観測から防御する防御手段中に内蔵されるようにしてもよい。

【００４５】また、暗号化関数が法ｐのもとでのＰｏｈｌｉｇ－Ｈｅｌｌｍａｎ非対称鍵暗号であり、アクセス資格認証の特徴情報が一方の鍵Ｄであり、鍵Ｄに対応する他方の鍵がＥであり（ＤＥ ｍｏｄ ｐ－１ ＝ １）、証明データ検証手段は、第５の記憶手段に書き込まれた証明データＲをＥ乗した結果と、第４の記憶手段に記憶されている認証用データＣとが法ｐのもとで合同であること（R^E ｍｏｄ ｐ ＝ Ｃ ｍｏｄ ｐ）を検証するようにしてもよい。

【００４６】また、暗号化関数が法ｐのもとでのＰｏｈｌｉｇ－Ｈｅｌｌｍａｎ非対称鍵暗号であり、アクセス資格認証の特徴情報が一方の鍵Ｄであり、鍵Ｄに対応する他方の鍵がＥであり（ＤＥ ｍｏｄ ｐ－１ ＝ １）、上記第７の記憶手段に記憶される認証用素データがデータＫを法ｐのもとでＥ乗した数Ｋ’（$=K^E$ ｍｏｄ ｐ）であり、上記乱数生成手段は、生成した乱数ｒを法ｐのもとでＥ乗した数と、前記Ｋ’とを法ｐのもとで乗じた数Ｃ（$=r^EK'$ ｍｏｄ ｐ）を認証用データとして前記第４の記憶手段に書き込み、証明データ検証手段は、第６の記憶手段に記憶されている乱数ｒの法ｐのもとでの逆数を、証明データ生成装置によって第５の記憶手段に書き込まれた証明データＲに乗じた数と、前記Ｋとが法ｐのもとで合同であること（Ｋ ｍｏｄ ｐ＝r^{-1}Ｒ ｍｏｄ ｐ）を検証するようにしてもよい。

【００４７】また、暗号化関数が法ｐのもとでのＰｏｈｌｉｇ－Ｈｅｌｌｍａｎ非対称鍵暗号であり、アクセス資格認証の特徴情報が一方の鍵Ｄであり、鍵Ｄに対応する他方の鍵がＥであり（ＤＥ ｍｏｄ ｐ－１ ＝ １）、上記第３の記憶手段に記憶される証明用補助情報ｔが、前記Ｄに、上記第２の記憶手段に記憶されるユーザ固有情報ｅと前記ｐとに依存する非衝突性関数値Ｆ（ｐ，ｅ）を加えて得られるデータ（ｔ＝Ｄ＋Ｆ（ｐ，ｅ））であり、上記証明データ生成手段は、前記ｔと、前記ｅと、第１の記憶手段に書き込まれた認証用データＣとから、法ｐのもとでＣのＤ乗（C^D ｍｏｄ ｐ）を計算することによって前記証明データを生成するようにしてもよい。

【００４８】また、上記証明データ生成手段が、第３の演算手段と、第４の演算手段と、第５の演算手段とからなり、第３の演算手段は、前記法ｐのもとで前記Ｃの前記ｔ乗（C^t ｍｏｄ ｐ）を計算し、第４の演算手段は、前記法ｐのもとで、前記Ｆ（ｐ，ｅ）を指数として、前記Ｃのべき乗（$C^{F(p,e)}$ ｍｏｄ ｐ）を計算し、第５の演算手段は、前記法ｐのもとで、第３の演算手段の計算結果と、第４の演算手段の計算結果の逆数とを乗じることによって、証明データＲ（$=C^tC^{-F(p,e)}$ ｍｏｄ ｐ）を生成するようにしてもよい。この場合にも、前記第２の記憶手段及び前記第４の演算手段が、内部の計算手順及びデータを外部の観測から防御する防御手段中に内蔵されるようにしてもよい。

【００４９】また、暗号化関数が法ｐ、生成元ａのもとでのＥｌＧａｍａｌ公開鍵暗号であり、アクセス資格認証の特徴情報が一方の鍵Ｘであり、鍵Ｘに対応する公開鍵がＹであり（Ｙ ＝ a^X ｍｏｄ ｐ）、ｕが上記ａを法ｐのもとで適当な乱数ｚを指数としてべき乗した数であり（ｕ＝a^z ｍｏｄ ｐ）、Ｋ’が、上記Ｙを法ｐのもとで上記乱数ｚを指数としてべき乗した数と、データＫとの積であるとき（Ｋ’＝Y^zK ｍｏｄ ｐ）、上記第７の記憶手段に認証用素データとしてｕ及びＫ’の組が記憶され、上記乱数生成手段は、上記ｕと、生成した乱数ｒを前記Ｋ’に法ｐのもとで乗じた数Ｃ（＝ｒＫ’ ｍｏｄ ｐ）とを認証用データとして前記第４の記憶手段に書き込み、証明データ検証手段は、第６の記憶手段に記憶されている乱数ｒの法ｐのもとでの逆数を、証明データ生成装置によって第５の記憶手段に書き込まれた証明データＲに乗じた数と、前記Ｋとが法ｐのもとで合同であること（Ｋ ｍｏｄ ｐ＝r^{-1}Ｒ ｍｏｄ ｐ）を検証するようにしてもよい。

【００５０】また、暗号化関数が法ｐ、生成元ａのもとでのＥｌＧａｍａｌ公開鍵暗号であり、アクセス資格認

証の特徴情報が一方の鍵Xであり、鍵Xに対応する公開鍵がYであり（$Y = a^X \mod p$）、上記第3の記憶手段に記憶される証明用補助情報tが、前記Xに、上記第2の記憶手段に記憶されるユーザ固有情報eと前記pとに依存する非衝突性関数値F（p，e）を加えて得られるデータ（t＝X＋F（p，e））であり、上記証明データ生成手段は、前記tと、前記eと、第1の記憶手段に書き込まれた認証用データu及びCから、法pのもとで、Cを上記uのX乗で割った数（$Cu^{-X} \mod p$）を計算することによって上記証明データを生成するようにしてもよい。

【００５１】また、上記証明データ生成手段が、第3の演算手段と、第4の演算手段と、第5の演算手段とからなり、第3の演算手段は、前記法pのもとで前記uの前記t乗（$u^t \mod p$）を計算し、第4の演算手段は、前記法pのもとで前記uの前記F（p，e）乗（$u^{F(p,e)} \mod n$）を計算し、第5の演算手段は、前記法pのもとで、上記Cを第3の演算手段の計算結果で割り、さらに、第4の演算手段の計算結果を乗じることによって、証明データR（$=Cu^{-t}u^{F(p,e)} \mod p$）を生成するようにしてもよい。この場合、前記第2の記憶手段及び前記第4の演算手段が、内部の計算手順及びデータを外部の観測から防御する防御手段中に内蔵されるようにしてもよい。

【００５２】また、署名関数が法p、生成元aのもとでのElGamal署名であり、アクセス資格認証の特徴情報が一方の鍵Xであり、鍵Xに対応する公開鍵がYであり（$Y = a^X \mod p$）、証明データ検証手段は、第5の記憶手段に書き込まれた証明データR及びSに対して、法pのもとで、上記aを第4の記憶手段に記憶されている認証用データCを指数としてべき乗した値と、上記YをR乗した値とRをS乗した値との積とが法pのもとで合同であること（$a^C \mod p = Y^R R^S \mod p$）を検証するようにしてもよい。

【００５３】また、署名関数が法p、生成元aのもとでのElGamal署名であり、アクセス資格認証の特徴情報が一方の鍵Xであり、鍵Xに対応する公開鍵がYであり（$Y = a^X \mod p$）、上記第3の記憶手段に記憶される証明用補助情報tが、前記Xに、上記第2の記憶手段に記憶されるユーザ固有情報eと前記pとに依存する非衝突性関数値F（p，e）を加えて得られるデータ（t＝X＋F（p，e））であり、上記証明データ生成手段は、証明データR及びSを生成するに当たり、適当な乱数kを生成し、法pのもとでの上記aのk乗をR（$=a^k \mod p$）とし、前記tと、前記eと、第1の記憶手段に書き込まれた認証用データCから、法p－1のもとで、CからXとrの積を引いた数にkの逆数を乗じることによって、S（$=(C-RX)k^{-1} \mod p-1$）を計算するようにしてもよい。この場合、第2の記憶手段及び証明データ生成手段が、内部の計算手順及びデータを外部の観測から防御する防御手段中に内蔵されるようにしてもよい。

【００５４】また、上記ユーザの固有情報が暗号関数の復号鍵であり、証明用補助情報がアクセス資格認証のための特徴情報を前記復号鍵に対応する暗号化鍵によって暗号化したものであり、第1の演算手段は上記ユーザの固有情報である復号鍵を用いて、証明用補助情報を復号することにより、アクセス資格認証のための特徴情報を算出するようにしてもよい。この場合、上記暗号関数が非対称鍵暗号関数であり、ユーザの固有情報が一方の鍵であってもよい。また、上記暗号関数が公開鍵暗号関数であり、ユーザの固有情報が秘密鍵であってもよい。また、記暗号関数が対称鍵暗号関数であり、ユーザの固有情報が共通秘密鍵であってもよい。

【００５５】また、上記証明データ検証手段は、さらに、暗号化されたデータである上記認証用データあるいは上記認証用素データに対応する平文データを記憶する第8の記憶手段と、比較手段とを有し、上記比較手段は、上記証明データ生成手段が生成した上記証明データ或は必要に応じて証明データから乱数効果を除去した結果と、第8の記憶手段に記憶されている平文データを比較し、両者が一致した場合に限り、上記証明データが正当であると判断するようにしてもよい。

【００５６】また、上記証明データ検証手段は、さらに、暗号化されたデータである上記認証用データあるいは上記認証用素データに対応する平文データに所定の一方向関数を施した結果を記憶する第9の記憶手段と、上記一方向関数を実行する第6の演算手段と、比較手段とを有し、第6の演算手段は、上記証明データ生成手段が生成した上記証明データに、必要ならば乱数効果を取り除いたのち、一方向関数を施し、上記比較手段は、第6の演算手段による計算結果と、第9の記憶手段に記憶されているデータを比較し、両者が一致した場合に限り、上記証明データが正当であると判断するようにしてもよい。

【００５７】また、上記証明データ検証手段は、さらに、プログラム実行手段を含み、上記認証用データあるいは上記認証用素データは、プログラムを暗号化して得られるデータであり、上記証明データ検証手段が、証明データ生成手段が生成した上記証明データを、必要ならば乱数効果を取り除いたのち、プログラムとしてプログラム実行手段に引き渡すことにより、証明データ生成手段が暗号化されたプログラムである上記認証用データあるいは認証用素データを正しく復号した場合、即ち、暗号化されたプログラムが正しく復号された場合に限り、プログラム実行手段が正しい動作を行うようにしてもよい。

【００５８】また、上記証明データ検証手段は、さらに、プログラム実行手段と、プログラム記憶手段と、プログラム復号手段とを含み、プログラム記憶手段に記憶

されているプログラムは、その一部あるいは全部が暗号化されたものであり、上記認証用データあるいは上記認証用素データは、前記暗号化されたプログラムを復号するための復号鍵を別途暗号化して得られるデータであり、上記証明データ検証手段は、証明データ生成手段が生成した上記証明データをプログラム復号手段に引き渡し、プログラム復号手段は、必要ならば乱数効果を取り除いたのち、前記証明データ生成手段が生成した証明データを復号鍵として用いることにより、プログラム記憶手段に記憶されたプログラムの必要な部分を復号し、プログラム実行手段が復号されたプログラムを実行することにより、証明データ生成手段が上記認証用データあるいは認証用素データを正しく復号された場合、即ち、暗号化されたプログラムを復号するために復号鍵が正しく復号された場合に限り、プログラム実行手段が正しい動作を行うようにしてもよい。

【００５９】また、上記証明データ生成装置および上記証明データ認証装置が同一の筐体内に設けられ、上記証明データ生成装置および上記証明データ認証装置が、当該筐体の外部の通信媒体を解さずに通信を行うようにしてもよい。

【００６０】また、この発明の第２の側面によれば、ユーザのアクセス資格を証明するために認証用データから生成された証明データの正当性を検証することにより上記ユーザのアクセス資格を認証するアクセス資格認証方法において、上記認証用データを記憶するステップと、ユーザの固有情報を記憶するステップと、上記ユーザの固有情報と、アクセス資格認証の特徴情報とに対し、所定の計算を実行した実行結果である証明用補助情報を記憶するステップと、上記認証用データと、上記ユーザの固有情報と、上記証明用補助情報とに所定の計算を施して証明データを生成するステップと、上記証明データ生成手段によって生成された証明データが上記アクセス資格認証の特徴情報に基づいて生成されていることを検証するステップとを実行するようにしている。

【００６１】また、この発明の第３の側面によれば、ユーザのアクセス資格を証明するために認証用データから生成された証明データの正当性を検証することにより上記ユーザのアクセス資格を認証するために、コンピュータで用いられるアクセス資格認証用プログラム製品において、上記認証用データを記憶するステップと、ユーザの固有情報を記憶するステップと、上記ユーザの固有情報と、アクセス資格認証の特徴情報とに対し、所定の計算を実行した実行結果である証明用補助情報を記憶するステップと、上記認証用データと、上記ユーザの固有情報と、上記証明用補助情報とに所定の計算を施して証明データを生成するステップと、上記証明データ生成手段によって生成された証明データが上記アクセス資格認証の特徴情報に基づいて生成されていることを検証するステップとを上記コンピュータに実行させるのに用いるようにしている。

【００６２】また、この発明の第４の側面によれば、ユーザのアクセス資格を認証するために正当性を検証される証明データを、認証用データから生成するために、コンピュータで用いられる証明データ生成用プログラム製品において、上記認証用データを記憶するステップと、ユーザのの固有情報を記憶するステップと、上記ユーザの固有情報と、アクセス資格認証の特徴情報とに対し、所定の計算を実行した実行結果である証明用補助情報を記憶するステップと、上記認証用データと、上記ユーザの固有情報と、上記証明用補助情報とに所定の計算を施して証明データを生成するステップとを上記コンピュータに実行させるのに用いるようにしている。

【００６３】また、この発明の第５の側面によれば、ユーザのアクセス資格を証明するために生成された証明データの正当性を検証することにより上記ユーザのアクセス資格を認証し、上記資格の認証に基づいてプログラムの実行を制御するプログラム実行制御装置に、認証用データを記憶する第１の記憶手段と、ユーザの固有情報を記憶する第２の記憶手段と、上記ユーザの固有情報と、アクセス資格認証の特徴情報とに対し、所定の計算を実行した実行結果である証明用補助情報を記憶する第３の記憶手段と、上記第２の記憶手段に記憶されている上記ユーザの固有情報と、上記第３の記憶手段に記憶されている上記証明用補助情報とを利用して、上記認証用データから上記証明データを生成する証明データ生成手段と、上記証明データ生成手段から生成された証明データの正当性を検証する手段と、上記証明データの正当性が検証されたときにプログラムの実行を継続する手段とを設けるようにしている。

【００６４】また、この発明の第６の側面によれば、所定の情報処理資源へのユーザのアクセス資格を証明するために生成された証明データの正当性を検証することにより上記ユーザのアクセス資格を認証して上記所定の情報処理資源へのアクセスを許容する情報処理装置に、認証用データを記憶する第１の記憶手段と、ユーザの固有情報を記憶する第２の記憶手段と、上記ユーザの固有情報と、アクセス資格認証の特徴情報とに対し、所定の計算を実行した実行結果である証明用補助情報を記憶する第３の記憶手段と、上記第２の記憶手段に記憶されている上記ユーザの固有情報と、上記第３の記憶手段に記憶されている上記証明用補助情報とを利用して、上記認証用データから上記証明データを生成する証明データ生成手段と、上記証明データ生成手段から生成された証明データの正当性を検証する手段と、上記正当性の検証に基づいて上記所定の情報処理資源へのアクセスを許可する手段とを設けるようにしている。

【００６５】

【発明の実施の態様】まず、この発明の原理的な構成例について説明する。この構成例のユーザ認証システム

は、アプリケーションの実行制御のみでなくメールのプライバシー保護やファイルや計算機資源等のアクセス制御にも適用できる。

【００６６】図１において、ユーザ認証システムは証明データ検証装置１０および証明データ生成装置１１からなっており、証明データ生成装置１１はアクセスチケット生成装置１２からアクセスチケット（証明用補助データ）１３を受領するようになっている。証明データ検証装置１０は検証ルーチン１５を実行する。証明データ生成装置１１はユーザ固有情報１６およびアクセスチケット１３を保持し、証明データ生成プログラム１７を実行する。

【００６７】アクセスチケット生成装置１２はアプリケーション作成者等のプロテクト側或は信頼できる第三者に設けられている。アクセスチケット生成装置１２はアクセス資格認証の特徴情報１４およびユーザ固有情報１６に基づいてアクセスチケット１３を生成し、このアクセスチケット１３が通信またはフロッピーディスケット等の送付を介してユーザに送られ、ユーザの証明データ生成装置１１に保持される。この後、証明データ検証装置１０は認証用データ１８を証明データ生成装置１１に送出する。証明データ生成装置１１はアクセスチケット１３およびユーザ固有情報１６を用いて証明データ１９を生成し、これを証明データ検証装置１０に返信する。証明データ検証装置１０は認証用データに基づいて証明データの正当性を検証する。すなわち、証明データが、認証用データとアクセス資格認証の特徴情報とに基づいて生成されたデータであることを検証する。

【００６８】証明データの正当性が検証されれば、ユーザのアクセス資格が認証され、これに応じて、プログラムの実行継続、ファイルへのアクセス等が許される。

【００６９】以上の構成について、アプリケーションプログラムの実行制御を例にとってさらに説明する。

【００７０】このような構成において、まず、アプリケーションプログラムのユーザはユーザ固有情報１６をただ一つ保持する。ユーザ固有情報は、パスワード認証におけるパスワードに相当するものであり、ユーザの身許を証明する唯一の重要な情報である。ユーザがユーザ固有情報１６をコピーして配布することができると、正当な利用権をもたないユーザにもアプリケーションプログラムの使用等を許すこととなるので、ユーザ固有情報１６はその正当な保持者であるユーザもこれを窃取することができないように、防御手段によって保護される。この防御手段は、プローブによる内部状態の窃取への防御力を有するハードウェア（以下、耐タンパーハードウェアと呼ぶ）により構成することができる。耐タンパーハードウェアの実現手法については後述する。

【００７１】また、ユーザには、上記ユーザ固有情報１６に加えて、所定の計算手続きを実行する証明データ生成プログラム１７が与えられる。このプログラム１７は、アプリケーション中のユーザ認証ルーチン（証明データ検証ルーチン１５）と通信を行なうためのものであり、ユーザ固有情報１６およびアクセスチケット１３のふたつのパラメータが与えられると、任意の入力値に対して計算を行ないユーザの身元を証明する証明データ１９を生成する。この計算の過程でユーザ固有情報１６が用いられるが、前に述べた理由によりユーザ固有情報１６が外部に漏洩すると問題があるため、上記プログラムの少なくとも一部は上記防御手段によって保護される必要がある。

【００７２】以下、上記防御手段によって保護されているユーザ固有情報記憶手段およびプログラムの一部と、該プログラム部分を実行するための装置（例えばメモリとＭＰＵにより構成される）と、上記防御手段とを併せてトークン（図１の符号２０で示す）と呼ぶこととする。トークンはＩＣカードのような可搬性を有する構成とすることもできる。

【００７３】一方、従来の実行制御技術と同様に、アプリケーションプログラム中には証明データ検証ルーチン１５が組み込まれる。証明データ検証ルーチン１５は、ユーザが保持する上記証明データ生成プログラム１７と通信し、返信結果（証明データ１９）が正しい場合に限りプログラムの実行を続行するように作成される点において、従来技術と同様である。従って、プログラム作成者は、送信データ（認証用データ１８）とそれに対する正しい返信データ（証明データ１９）の組合せを計算する方法を知っている必要がある。

【００７４】証明データ検証ルーチン１５の作用を以下に数例述べる。

１．証明データ検証ルーチン１５中には、送信するべきデータ（認証用データ１８）と期待される返信データ（期待値）が埋入されている。証明データ検証ルーチン１５は上記送信データを取り出してユーザに送信し、ユーザから返信を受け取る。次いで、ユーザからの返信データと上記期待値とを比較し、両者が一致した場合はプログラムの次のステップを実行し、一致しない場合はプログラムの実行を停止する。

【００７５】ここで、返信データが送信データの所定の暗号化アルゴリズムに従う暗号化の結果であるとした場合には、アクセス資格認証の特徴情報は暗号化鍵となる。

【００７６】２．証明データ検証ルーチン１５中には、送信するべきデータと、期待される返信データに一方向関数を施したデータ（期待値）が埋入されている。証明データ検証ルーチン１５は上記送信データを取り出してユーザに送信し、ユーザから返信を受け取る。次いで、ユーザからの返信データに上記一方向関数を施した値を、上記期待値と比較し、両者が一致した場合はプログラムの次のステップを実行し、一致しない場合はプログラムの実行を停止する。

【００７７】ここで、返信データが送信データの所定の暗号化アルゴリズムに従う暗号化の結果であるとした場合には、アクセス資格認証の特徴情報は暗号化鍵となる。

【００７８】３．アプリケーションプログラムのコードの一部を予め定められた暗号化アルゴリズムに従って暗号化しておくことにより、該プログラムの実行が不可能となるようにするプロテクトを施す。証明データ検証ルーチン１５は、上記暗号化されたコードをユーザに送信し、その返信として受け取った値を暗号化以前のコードと置き換える手続きを行なう。

【００７９】以上の構成によると、返信データが暗号化されたコードの正しい復号である場合に限り、該プログラムの実行が可能となる。この場合のアクセス資格認証の特徴情報は暗号化されたコードを復号するための復号鍵となる。

【００８０】４．アプリケーションプログラムのコードの一部を予め定められた暗号化アルゴリズムに従って暗号化しておくことにより、該プログラムの実行が不可能となるようにするプロテクトを施す。更に、上記コードの暗号化に用いた暗号化鍵と対をなす復号鍵を別途暗号化したデータを送信データとして証明データ検証ルーチン１５中に埋入しておく。証明データ検証ルーチン１５は、上記暗号化された復号鍵をユーザに送信し、その返信として受け取った値を復号鍵として、上記暗号化されたコードを復号する。

【００８１】以上の構成によると、返信データが正しく復号された復号鍵である場合にかぎって、上記暗号化されたコードは正しく復号され、該プログラムの実行が可能となる。この場合のアクセス資格認証の特徴情報は暗号化された復号鍵を復号するための復号鍵となる。

【００８２】さて、従来の実行制御技術では、ユーザ固有情報（ユーザの認証鍵）がアクセス資格認証の特徴情報と同一である。従来の証明データ生成ルーチンはアクセス資格認証の特徴情報と証明データ検証ルーチンから送信されたデータとを入力として、返信データを計算する。

【００８３】これに対し、この発明の特徴は、ユーザ固有情報１６とアクセス資格認証の特徴情報１４とが互いに独立である点にある。この構成例でも、証明データ生成プログラム１７は、ユーザ固有情報１６と証明データ検証ルーチン１５から送信されたデータ（認証用データ１８）に加えて、アクセスチケット１３を入力として、返信データ（証明データ１９）を計算する。この構成は以下の性質をもつ。

【００８４】１．アクセスチケット１３は特定のユーザ固有情報１６とアクセス資格認証の特徴情報１４とに基づいて計算されるデータである。

２．ユーザ固有情報１６を知らずにアクセスチケット１３からアクセス資格認証の特徴情報１４を計算することは少なくとも計算量的に不可能である。

３．証明データ生成プログラム１７はユーザ固有情報１６とアクセスチケット１３との正しい組合せ、即ち、ユーザ固有情報１６と該ユーザ固有情報１６に基づいて計算されたアクセスチケット１３の組合せが入力された場合に限って、正しい返信データを計算する。

【００８５】以上により、ユーザはあらかじめユーザ固有情報１６を所持し、プログラム作成者はユーザが所持するユーザ固有情報１６とは独立にアプリケーションプログラムを作成し、アクセスチケット１３をユーザ固有情報１６とアプリケーションプログラムの作成に使用したアクセス資格認証の特徴情報１４とに応じて作成し、配布することにより、実行制御を行なうことができる。

【００８６】また、ユーザ固有情報１６を二つの固有情報からなるものとし、アクセスチケット１３の作成に際して用いる固有情報と、ユーザが通信プログラムにおいて用いる固有情報とを区別して用いることもできる。最も典型的な例は、ユーザ固有情報１６を公開鍵ペアとし、公開鍵を公開してアクセスチケット作成に用い、個人鍵をユーザ個人の秘密情報としてトークン２０中に封入しておく方法である。この場合は、アクセスチケット１３をアクセス資格認証の特徴情報１４と上記公開鍵ペアの公開鍵から計算できるようにすることにより、ユーザ固有情報１６を秘密に保ったままアクセスチケット１３を計算することが可能となる。

【００８７】

【実施例】つぎにより具体的な構成について実施例に即して説明する。

［全体構成］

【００８８】具体的な個別の実施例を述べる前に、この発明の実施形態の全体像を以下に述べる。

【００８９】まず、この発明を、ユーザのＰＣあるいはワークステーション上で動作するアプリケーションプログラムの実行制御に用いる場合について述べる。図２はこの実施形態における装置の全体構成を示す。なお、図２において図１と対応する箇所には対応する符号を付して詳細な説明は繰り返さない。

【００９０】この実施形態においては、証明データ生成装置１１はユーザが用いる計算機３１上の証明用プログラム３２として実現することができる。この際、ユーザを識別するための固有情報（ユーザ固有情報）の安全性を高めるために、該計算機３１に装着され、耐タンパー特性を有する証明用ハードウェア３３（ＩＣカード、ボードなど）を併用することも可能である。この際、ＩＣカードのような携帯性のあるハードウェアを用いれば、ユーザが複数のＰＣあるいはワークステーション上で作業をする場合に便利である。

【００９１】証明データ検証装置１０は該ユーザが利用するアプリケーションプログラム３４の一部として構成される。即ち、ユーザが該アプリケーションプログラム

３４をＰＣあるいはワークステーション上で起動すると、該アプリケーションプログラム３４中にプログラムとして記述された証明データ検証装置１０が起動され、証明データ生成装置１１と通信してユーザ認証を行ない、通信が正しく終了した場合に限って該アプリケーションプログラムの実行を可能とする。

【００９２】ユーザが、証明データ検証装置１０が埋めこまれた前記アプリケーションプログラム３４を利用するためには、ユーザ本人宛に発行され、前記アプリケーションプログラムに対応する証明用補助情報（アクセスチケット）を取得する必要がある。ユーザは、前記ＰＣあるいはワークステーション上にインストールされた証明用プログラム３２に、取得したアクセスチケットを登録するとともに、例えば、ユーザ固有情報がＩＣカードに封入されている場合には、ＩＣカードを前記ＰＣあるいはワークステーションに装着する。

【００９３】証明データ生成装置１１（ＰＣあるいはワークステーション上のプログラムとＩＣカードによって構成される）は、ユーザ固有情報とアクセスチケットに基づいて計算を行い、その計算に基づいて証明データ検証装置１０と通信を行う。

【００９４】通信の結果、証明データ検証装置１０による認証が成功するのは、ユーザ固有情報と、アクセスチケットと、証明データ検証装置１０が埋めこまれた前記アプリケーションプログラム３４の三つが正しく対応している場合に限る。

【００９５】ユーザ固有情報あるいはアクセスチケットの一方が欠けていた場合には、認証は成功しない。

【００９６】アクセスチケットは特定のユーザ宛に発行される。即ち、アクセスチケットの生成に際して、特定のユーザのユーザ固有情報が使用される。アクセスチケット生成時に使用されるユーザ固有情報と、証明データ生成装置１１によって使用される前記ユーザ固有情報とが一致していない場合、やはり、認証は成功しない。

【００９７】また、アクセスチケットは、特定のアクセス資格認証の特徴情報に基づいて生成され、証明データ検証装置１０はこのアクセス資格認証の特徴情報を認証するように構成される。従って、アクセスチケットの生成のもととなった特徴情報と、アプリケーションプログラム３４に埋めこまれている証明データ検証装置１０が認証しようとする特徴情報とが互いに対応していなかった場合にも、認証は成功しない。

【００９８】なお、図2において、３５はオペレーティング・システム等の制御プログラムであり、３６はハードウェア全般を示す。

【００９９】また、アプリケーションプログラム３４がネットワークによって結合された別の計算機上で実行され、実行結果がネットワークを介してユーザが用いる計算機に通信されるものとしてもよい。この場合、いわゆるサーバ・クライアントモデルに基づく構成となる。先に述べた、ユーザのＰＣあるいはワークステーション上で実行されるアプリケーションプログラムの実行制御の場合では、証明データ生成装置１１と証明データ検証装置１０との通信がいわゆるプロセス間通信として実行されるのに対し、サーバ・クライアント・モデルに従った場合、証明データ生成装置１１と証明データ検証装置１０との通信はＴＣＰ／ＩＰなどのネットワークプロトコルに従った通信として実行される。

【０１００】また、アプリケーションプログラムが専用装置上に構成されている場合にも、この発明を適用することが可能である。例えば、証明データ生成装置全体をＩＣカード内に実装し、取得したアクセスチケットもＩＣカードに登録するものとする。証明データ検証装置は前記専用装置上に実装されるが、該専用装置はＩＣカードを挿入するためのスロットを備え、ユーザは該スロットに所有するＩＣカードを挿入することで認証を行う。このような専用装置による構成は、銀行のＡＴＭ機や、ゲームセンターにおけるゲーム機などに適用することができる。

【０１０１】ユーザによるアクセスチケットの取得に関しては、共通のセンターがユーザからの発行依頼に応じて生成して配布する方法と、アプリケーションプログラムの作成者が、アクセスチケット発行プログラムやアクセスチケット生成装置の助けを借りて個別に生成する方法がある。

【０１０２】生成されたアクセスチケットは、フロッピーディスク等の可搬型記憶媒体を介してユーザに配送されるものとしてもよいが、アクセスチケットが十分な安全性を備えていることから、電子メールなどを用いてネットワークを介して配送されるように構成してもよい。

【０１０３】アクセスチケットの安全性とは、以下の二つの性質である。

【０１０４】アクセスチケットは記名式であり、即ち、アクセスチケットが発行されたユーザ本人（正確には、アクセスチケット生成時に用いられたユーザ固有情報の保持者）だけが該アクセスチケットを用いて証明データ生成装置を正しく作動させることができる。従って、悪意の第三者がネットワークを盗聴し、他のユーザのアクセスチケットを不正に手に入れたとしても、この第三者がアクセスチケットの発行先である正規のユーザのユーザ固有情報を手に入れないかぎり、このアクセスチケットを利用することは不可能である。

【０１０５】アクセスチケットはさらに厳密な安全性を保持している。即ち、悪意の第三者が任意個数のアクセスチケットを集めて、いかなる解析を行ったとしても、得られた情報をもとに別のアクセスチケットを偽造したり、証明データ生成装置の動作を模倣して認証を成立させるような装置を構成することは不可能である。

【０１０６】以下では、より具体的な構成について実施例に即して説明する。

［第一の実施例］

【0107】この発明における第一の実施例では、アクセスチケットｔは次の式１に基づいて生成されるデータである。

【数１】（１）　　ｔ　＝　Ｄ－ｅ＋ωφ（ｎ）

上式中の各記号は以下を表す。

【0108】ｎはＲＳＡ法数、即ち、十分大きな二つの素数ｐ、ｑの積である（ｎ＝ｐｑ）。

【0109】φ（ｎ）はｎのオイラー数、即ち、ｐ－１とｑ－１の積である（φ（ｎ）＝（ｐ－１）（ｑ－１））。

【0110】ユーザ固有情報ｅは、ユーザ毎に異なる数であり、ユーザを識別するために用いられる。

【0111】アクセスチケット秘密鍵Ｄは、法数ｎのもとでのＲＳＡ秘密鍵であり、式２を満たす。

【数２】（２）　　ｇｃｄ（Ｄ，φ（ｎ））＝１

ここで、ｇｃｄ（ｘ，ｙ）は二数ｘ、ｙの最大公約数を表す。式（２）によって表現される性質は、式３を満たす数Ｅが存在することを保証する。

【数３】

（３）　　ＥＤ　ｍｏｄ　φ（ｎ）　＝　１

Ｅをアクセスチケット公開鍵と呼ぶ。

【0112】ωは、ｎ及びｅに依存して定まる数であり、ｎあるいはｅのいずれか一方が異なる場合、その値が容易に一致しない（衝突しない）ように定める。ωの定め方の一例として、一方向ハッシュ関数ｈを利用して、式４のようにωを定める方法もある。

【数４】（４）　　ω＝ｈ（ｎ｜ｅ）

ただし、記号｜はビット列の接合を表す。

【0113】一方向ハッシュ関数とは、ｈ（ｘ）＝ｈ（ｙ）を満たす相異なるｘ、ｙを算出することが著しく困難であるという性質をもつ関数である。一方向ハッシュ関数の例として、ＲＳＡ　Ｄａｔａ　Ｓｅｃｕｒｉｔｙ　Ｉｎｃ．によるＭＤ２、ＭＤ４、ＭＤ５、米国連邦政府による規格ＳＨＳ（Ｓｅｃｕｒｅ　Ｈａｓｈ　Ｓｔａｎｄａｒｄ）が知られている。

【0114】上記の説明中に現れた数において、ｔ、Ｅ、ｎは公開可能であり、残りのＤ、ｅ、ω、ｐ、ｑ、φ（ｎ）はチケットを作成する権利を有する者以外には秘密である必要がある。図を参照してさらに第一の実施例について詳細に説明する。図３は、この発明における第一の実施例の構成を示し、図４は図３におけるデータのフローを示している。図３において、証明データ検証装置１０は、アクセスチケット公開鍵記憶部１０１、乱数発生部１０２、乱数記憶部１０３、受信データ記憶部１０５、検証部１０６、実行部１０７およびエラー処理部１０８を含んで構成されている。また、証明データ生成装置１１は、受信データ記憶部１１１、第１演算部１１２、アクセスチケット記憶部１１３、第２演算部１１４、ユーザ固有情報記憶部１１５および証明データ生成部１１６を含んで構成されている。

【0115】つぎに動作について説明する。

１．ユーザがアクセスすることによって、証明データ検証装置１０１が起動される。証明データ検証装置１０の起動に関しては以下のような形態が考えられる。

【0116】証明データ検証装置１０がユーザのＰＣあるいはワークステーション上で動作するアプリケーションプログラムの一部として構成されている場合、ユーザがキーボードあるいはマウスなどの指示装置を用いた通常の方法で、該アプリケーションプログラムを起動する。アプリケーションプログラムの実行が証明データ検証装置１０を構成しているプログラムに到達することによりことにより、証明データ検証装置１０が起動される。

【0117】証明データ検証装置１０がネットワークで結ばれた他のＰＣあるいはワークステーション（サーバと呼ぶ）上に構成されてい場合、ユーザは自分のＰＣあるいはワークステーション上の通信プログラムを起動し、該通信プログラムが所定の手続きに従って前記サーバに通信の開設要求を行うことにより、証明データ検証装置１０が起動される。例えば、ユーザの通信プログラムがサーバと通信する際にＴＣＰ／ＩＰと呼ばれる手続きに従うとすると、証明データ検証装置をサーバの特定のポートに予め対応づけておき、更に、ユーザの通信プログラムが該ポートを指定してＴＣＰ接続要求をサーバに要求するように設定しておくことにより、サーバ上のデーモン（ｉｎｅｔｄ）がＴＣＰ接続要求に応じて証明データ検証装置１０を起動することが可能となる。このような実現方法は、インターネットなどのネットワークにおいて広く利用されているものである。

【0118】証明データ検証装置１０を専用目的の装置とすることも可能である。例えば、証明データ検証装置１０をＩＣカード・リーダ・ライター内のＲＯＭに焼きつけられたプログラムあるいはＥＥＰＲＯＭに書き込まれたプログラムとして構成し、証明データ生成装置１１をＩＣカードのマイクロコントローラーに実装されたプログラムとすることができる。この場合、ユーザがＩＣカードをリーダ・ライターに挿入することにより、証明データ検証装置１０が起動される。

【0119】２．証明データ検証装置１０は、認証用データＣとアクセスチケット公開鍵記憶部１０１に記憶されているＲＳＡ暗号の法数ｎとを、証明データ生成装置１１中の受信データ記憶部１１１に書き込むが、この認証用データＣは以下の方法で生成される。

【0120】証明データ検証装置中の乱数発生部１０２によって，乱数ｒを、アクセスチケット公開鍵記憶部１０１に保持されているＲＳＡ法数ｎと互いに素になるように生成し、乱数記憶部１０３に記録する。更に、この乱数ｒを認証用データＣとする。後述するように、この場合、証明データ生成装置１１が返す証明データは、Ｃ

を法数nののもとでRSA暗号を用いて暗号化したものとなる。

【0121】Cの値は乱数rそのものであることから、通信の度に異なる値となり、リプレイアタックを防止する効果をもつ。

【0122】3．証明データ生成装置11中の第1演算部112は、アクセスチケット記憶部113に記憶されているアクセスチケットtを取得し、受信データ記憶部111に書き込まれたRSA法数nのもとで、式5を実行し中間情報R'を得る。

【数5】（5）　$R' = C^t \mod n$

【0123】4．証明データ生成装置11中の第2演算部114は、ユーザ固有情報記憶部115に記憶されているユーザの固有情報eを取得し、式6の計算を実行し差分情報Sを得る。

【数6】（6）　$S = C^e \mod n$

5．証明データ生成装置11中の証明データ生成部116は、第1および第2演算部112、114からR'およびSを得て、式7の計算を行ないRを得る。

【数7】（7）　$R = R' S \mod n$

【0124】6．証明データ生成装置11はRを証明データ検証装置10の受信データ記憶部105に返送する。

【0125】7．証明データ検証装置10中の検証部106は、まず、受信データ記憶部105に返された証明データRと、アクセスチケット公開鍵記憶部101に保持されている公開指数EおよびRSA法数nをもとに式8の計算を行なう。

【数8】（8）　$R^E \mod n$

次いで、この計算結果と、乱数記憶部103中に保持されている乱数C（＝r）とを比較することにより、式9が成り立つことを確かめる。

【数9】

（9）　$C \mod n = R^E \mod n$

式（9）が成立する場合は実行部107を起動して処理を継続し、成立しない場合はエラー処理部108を起動してエラー処理を行う。

【0126】［第二の実施例］この発明の第二の実施例における、アクセスチケットtの構成、証明データ証明装置の作用は、前記第一の実施例におけるそれと同一である。第一の実施例においては証明データは認証用データの暗号化であったのに対し、第二の実施例においては証明データ検証装置10が生成する認証用データは証明データの（乱数効果付）暗号化であり、証明データ生成装置11は認証用データを復号して（乱数効果を維持したまま）証明データを生成する。図を参照してさらに第二の実施例について詳細に説明する。図5は、この発明における第二の実施例の構成を示し、図6は図5におけるデータのフローを示している。図5において、証明データ検証装置10は、アクセスチケット公開鍵記憶部101、乱数発生部102、乱数記憶部103、受信データ記憶部105、乱数化部121、認証用素データ記憶部122、乱数効果除去部123、および実行手段310を含んで構成されている。また、証明データ生成装置11は、受信データ記憶部111、第1演算部112、アクセスチケット記憶部113、第2演算部114、ユーザ固有情報記憶部115および証明データ生成部116を含んで構成されている。

【0127】つぎに動作について説明する。

1．ユーザがアクセスすることによって、証明データ検証装置10が起動される。

【0128】証明データ検証装置の実現方法として、ユーザのPCやワークステーション上で動作するアプリケーションプログラム、ユーザのPCやワークステーションとネットワークを介して接続されたサーバ上のサーバプログラム、あるいは、ICカード・リーダ・ライターのような専用の装置のいずれも可能であることは、第一の実施例の場合と変わらない。

【0129】2．証明データ検証装置10は、認証用データCと、アクセスチケット公開鍵記憶部101に保持されているRSA暗号の法数nとの組を証明データ生成装置11中の受信データ記憶部111に書き込むが、認証用データCは以下の方法で生成される。

【0130】証明データ検証装置中の乱数発生部102によって、乱数rをアクセスチケット公開鍵記憶部101に保持されているRSA法数nと互いに素になるように生成し、乱数記憶部103に記録する。乱数化部121は、アクセスチケット公開鍵記憶部101に格納されている公開指数Eと法数nを取得し、さらに認証用素データ記憶部122に記憶されているデータC'を取得して、式10の計算を行なう。

【数10】（10）　$C = r^E C' \mod n$

ここで、認証用素データC'はデータKに対して関係式11を満たすように生成され、認証用素データ記憶部122に格納された値である。

【数11】（11）　$C' = K^E \mod n$

ここで、データKを証明データ検証装置に保持せず、代わりに、その暗号化の結果であるC'のみを保持するように証明データ検証装置10を構成すれば、証明データ検証装置10からデータKが漏洩する危険を回避することができる。

【0131】基本的に見れば、認証用データCは法数nのもとでRSA暗号を用いてデータKを暗号化したものであり、証明データ生成装置11はCを法数nのもとでRSA暗号を用いて復号することによりデータKを再現する。しかし、このままでは、証明データ検証装置10と証明データ生成装置11の間の通信は常に同一のものとなり、いわゆるリプレイアタックが可能となることから、乱数rを用いて認証用データに乱数効果を与え、証明データ生成装置11が返すデータを検証する際に乱数

効果を除去するように構成される。

【0132】3．証明データ生成装置11中の第1演算部112は、アクセスチケット記憶部113に記憶されているアクセスチケットtを取得し、受信データ記憶部111に書き込まれたRSA法数nのもとで式12を実行し中間情報R'を得る。

【数12】（12）　$R' = C^t \mod n$

【0133】4．証明データ生成装置11中の第2演算部114は、ユーザ固有情報記憶部115に記憶されているユーザの固有情報eを取得し、式13の計算を実行し差分情報Sを得る。

【数13】（13）　$S = C^e \mod n$

5．証明データ生成装置11中の証明データ生成部116は、第1および第2演算部112、114からR'およびSを得て、式14の計算を行ないRを得る。

【数14】（14）　$R = R'S \mod n$

【0134】6．証明データ生成装置11はRを証明データ検証装置10の受信データ記憶部105に返送する。

【0135】7．証明データ検証装置10中の乱数効果除去部123は、乱数記憶部103中から先に生成した乱数rと、受信データ記憶部106から証明データRとを取り出し、式15の計算を行なう。

【数15】（15）　$K' = r^{-1}R \mod n$

証明データ生成装置11において用いられるアクセスチケットtとユーザの固有情報eの組合せが正しい場合に限り、計算の結果得られたK'とKが一致することに注意せよ。

【0136】計算されたK'は、証明データ検証装置10中の実行手段310に引き渡されるが、実行手段310はK'＝Kが成立する場合に限り正規の処理を実行するように構成される。

【0137】以下に、証明データ検証装置10中の実行手段310の構成法を数例述べる。

【0138】1．図7の構成例

実行手段310中の記憶部310aに予めデータKを記憶しておく。実行部310中の比較部310bは、このKと証明データ生成装置11から送られた証明データRから乱数効果を除去して得られるK'とを直接比較し、K'＝Kが成立する場合に限り正規の処理を実行し、成立しない場合には処理を中止するなどのエラー処理を実行する（図8）。

【0139】この構成例には、検証に用いるデータKが装置中に現れるという安全上の弱点がある。例えば、証明データ検証装置10、特に、実行手段310が、ユーザのPCあるいはワークステーション上で動作するプログラムとして構成されている場合、プログラムを解析してKを窃取することは、困難であっても、必ずしも不可能ではない。Kの値がユーザの知るところとなり、更に、証明データ検証装置で生成される乱数が予想可能であると、証明データ生成装置の動作を模倣する装置を構成することが可能となり、なりすましによる不正アクセスが可能となる。

【0140】2．図9の構成例

上記の欠点を改善するため、記憶部310aに記憶されるデータをKそのものではなく、Kに前述の一方向ハッシュ関数hを施して得られるデータh（K）とすることもできる。一方向ハッシュ関数の性質から、記憶部310aに記憶されるデータyから、y＝h（x）を満たすxを算出することは著しく困難である。

【0141】実行部310は、入力データに対し一方向ハッシュ関数を施した結果を返す変換部310cを有する。比較部310bは、上記変換部310cの出力h（K'）と、記憶部310aに記憶されたデータ（＝h（K））とを比較する（図10）。

【0142】この方法例では、検証に用いるデータKがプログラム中に現れることがなく、また、記憶部310aに記憶されたh（K）からKを計算することが著しく困難であることから、図7の例より安全であるといえる。

【0143】この構成では、図10に示すようにプログラムの実行を制御する。

【0144】しかしながら、比較部310bはプログラム中では条件文として構成され、証明データ検証装置10、特に、実行手段310がユーザのPCあるいはワークステーション上で動作するプログラムであるような場合、即ち、プログラムの分析・改竄が比較的容易であるような構成では、該条件文をスキップするようにプログラムを改竄することが可能である点で、なお弱点を有している。

【0145】3．図11の構成例

第3の構成例では、証明データ検証装置10の実行部310のプログラムのコードの一部或は全部を暗号化したデータを認証用素データC'として、認証用素データ記憶部122に保持する。即ち、Kは実行部プログラムのコードの一部或は全部である。

【0146】実行手段310は、証明データ生成装置11からの返信データから乱数効果を除去して得られるデータK'を、プログラム中の予め定められた位置に埋め込む。すなわち実行手段310は、コードとしてのデータK'を記憶するコード記憶部310dとこのコードをプログラム中に取り込むコード取り込み部310eと、プログラムを実行するコード実行部310fとを有している。証明データ生成装置11が正しいデータを返信した場合、即ち、K'＝Kである場合に限ってプログラムは実行可能となる（図12）。

【0147】この構成例では、プログラムの実行に不可欠なコードの一部或は全部が暗号化されているため、実行手段310がユーザのPCあるいはワークステーション上で動作するアプリケーションプログラムとして構成

されているような比較的安全性の低い場合でも、不正実行を防止することができる。

【０１４８】実行手段３１０がユーザのＰＣあるいはワークステーション上で動作するアプリケーションプログラムとして構成されている場合を例にとって、更に詳細な構成を述べる。

【０１４９】証明データが書き込まれるコード記憶部３１０ｄは、計算機中の指定された記憶領域である。

【０１５０】コード実行部３１０ｆは計算機のＣＰＵ及びＯＳである。ＣＰＵとＯＳとは協力して、計算機のプログラム領域に記憶されている実行命令を順に実行する。特定の機能を提供する一連の実行命令をプログラムコードと呼ぶ。

【０１５１】コード取込み部３１０ｅの実体は、実行手段３１０中で最初に実行されるプログラムコードである。コード取込み部３１０ｅは、直接・間接にコード記憶部３１０ｄのアドレスをコード実行部３１０ｆに指示することが可能である。例えば、コード取込み部３１０ｅはコード記憶部３１０ｄの物理アドレスを直接コード実行部３１０ｆに指示してもよいし、計算機のＯＳが仮想アドレッシングを実行する場合には、コード取込み部３１０ｅはコード記憶部３１０ｄの仮想アドレスを指示し、ＯＳがＣＰＵ経由で受け取った仮想アドレスを物理アドレスに変換する方法でもよい。

【０１５２】コード記憶部３１０ｄに証明データが書き込まれた状態で、プログラムであるコード取込み部３１０ｅが起動されると、コード取込み部３１０ｅは、コード記憶部３１０ｄのアドレスに記憶されている内容を計算機上のプログラム領域の特定のアドレスに書き出すよう、コード実行部３１０ｆに命令し、実行させる。

【０１５３】次いで、コード取込み部３１０ｅは、コード実行部３１０ｆに命令してコード記憶部３１０ｄの記憶内容を書き出させた、プログラム領域中の特定のアドレスの実行命令を実行するよう、ＪＭＰ命令等を用いてコード実行部３１０ｆに命令する。

【０１５４】この構成例では、証明データが証明データ生成装置１１によって正しく生成されたならば、乱数効果を取り除いた後のデータはプログラムコード、即ち、コード実行部３１０ｆへの一連の実行命令である。従って、上記構成では、コード取込み部３１０ｅのプログラムコードに引続き、証明データ生成手段１１によって復号されたプログラムコードが実行されることとなる。

【０１５５】４．図１３の構成例

第３の構成例において、暗号化したコードを復号するために必要な復号鍵を、Ｋとすることもできる。この構成によると、暗号化するコードのサイズに関わらず、Ｋのサイズ、すなわち認証用素データＣ’のサイズを一定の小さい値に抑えることが可能となり、通信のオーバヘッドを減少させることができる。

【０１５６】実行部３１０は、証明データ生成装置１１からの返信データから乱数効果を除去して得られるデータＫ’を用いて、プログラム中の予め定められた領域のコードを復号する。すなわち実行部３１０は暗号化されたプログラムを記憶するプログラム記憶部３１０ｇと、暗号化されたプログラムを読み出しデータＫ’を利用して復号する復号部３１０ｈと、復号されたコードを取り出すコード取り出し部３１０ｉと、取り出されたコードを実行するコード実行部３１０ｆとを有する。

【０１５７】実行手段３１０がユーザのＰＣあるいはワークステーション上で動作するアプリケーションプログラムとして構成されている場合を例にとって、更に詳細な構成を述べる。

【０１５８】暗号化されたプログラムコードが記憶されているプログラム記憶部３１０ｇは、計算機中の指定された記憶領域である。

【０１５９】コード実行部３１０ｆは計算機のＣＰＵ及びＯＳである。

【０１６０】プログラム記憶部３１０ｇは、ハードディスク等、補助記憶装置上のファイル領域であるとすることができる。即ち、暗号化されたプログラムコードは、ファイルとして記憶されている。

【０１６１】復号部３１０ｈの実体は、実行手段３１０中で最初に実行されるプログラムコードである。復号部３１０ｈは、直接・間接に、プログラム記憶部３１０ｇのアドレスを、コード実行部３１０ｆに指示することが可能である。

【０１６２】Ｋ’が与えられた状態で、プログラムである復号部３１０ｈが起動されると、復号部３１０ｈは、プログラム記憶部３１０ｇに記憶されているデータを順に、あるいは定められた長さのブロック毎に読み出し、そのデータにＫ’を復号鍵とした所定の復号処理を実行し、その復号結果を計算機上のプログラム領域の特定のアドレスに書き出すよう、コード実行部３１０ｆに命令し、実行させる。この処理により、プログラム記憶部３１０ｇに記憶されていた暗号化データに対し、Ｋ’を復号鍵として、所定の復号アルゴリズムを実行した結果を、プログラム領域中の特定の位置に書き込んだこととなる。

【０１６３】次いで、復号部３１０ｈは、コード実行部３１０ｆに命令して復号したプログラムコードを書き出させた、プログラム領域中の特定のアドレスの実行命令を実行するよう、ＪＭＰ命令等を用いてコード実行部３１０ｆに命令する。

【０１６４】この構成例では、証明データが証明データ生成装置１１によって正しく生成されたならば、乱数効果を取り除いたのちの値はプログラム記憶部３１０ｇに記憶されている暗号化されたプログラムコードを正しく復号するための復号鍵となる。復号部３１０ｈは、この復号鍵を用いて、前記暗号化プログラムコードを復号し、復号結果であるプログラムコードをプログラム領域

にロードし、ロードされた前記プログラムコードを実行するようコード実行部３１０ｆに命令する。従って、上記構成では、復号部３１０ｈのプログラムコードに引続き、証明データ生成手段１１によって復号された復号鍵を用いて復号されたプログラムコードが実行されることとなる（図１４）。

［第三の実施例］

【０１６５】この発明における第三の実施例では、アクセスチケットｔは次の式１６に基づいて生成されるデータである。

【数１６】

（１６）　　$t = D+F(n, e)$

上式中の各記号は以下を表す。

【０１６６】ｎはＲＳＡ法数、即ち、十分大きな二つの

（１８）　　$ED \mod \phi(n) = 1$

Ｅをアクセスチケット公開鍵と呼ぶ。

【０１７０】二変数関数Ｆ（ｘ，ｙ）は関数値が衝突しにくい二変数関数であり、例えば、前述の一方向ハッシュ関数ｈを利用して、式１９のように定めることができる。

【数１９】

（１９）　　$F(x, y)=h(x \mid y)$

図を参照してさらに第二の実施例について詳細に説明する。図１５は、この発明における第三の実施例の構成を示し、図１６は図１５におけるデータのフローを示している。図１５において、証明データ生成装置１１は、受信データ記憶部１１１、第１演算部１１２、アクセスチケット記憶部１１３、第２演算部１１４、ユーザ固有情報記憶部１１５、証明データ生成部１１６および指数生成部１３０を含んで構成されている。証明データ検証装置１０は第一の実施例（図３）や第二の実施例（図５）の構成を採用することができる。ここでは説明を繰り返さない。

【０１７１】つぎにこの構成における動作について説明する。

１．ユーザがアクセスすることによって、証明データ検証装置１０が起動される。

【０１７２】証明データ検証装置１０の実現方法として、ユーザのＰＣやワークステーション上で動作するアプリケーションプログラム、ユーザのＰＣやワークステーションとネットワークを介して接続されたサーバ上のサーバプログラム、あるいは、ＩＣカード・リーダ・ライターのような専用の装置のいずれも可能であることは、第一および第二の実施例の場合と変わらない。

【０１７３】２．証明データ検証装置１０は、認証用データＣとアクセスチケット公開鍵記憶部１０１に記憶されているＲＳＡ暗号の法数ｎとの組を証明データ生成装置１１中の受信データ記憶部１１１に書き込む。

【０１７４】Ｃの生成方法としては、第一の実施例で述べた方法、第二の実施例で述べた方法のいずれも適用可能であるので、ここでは特に限定しない。前記いずれかの方法で生成されたＣが証明データ生成装置１１中の受信データ記憶部１１１に書き込まれるものとする。

【０１７５】３．証明データ生成装置１１中の第１演算部１１２は、アクセスチケット記憶部１１３に記憶されているアクセスチケットｔを取得し、受信データ記憶部１１１に書き込まれたＲＳＡ法数ｎのもとで式２０を実行し中間情報Ｒ’を得る。

【数２０】（２０）　　$R' = C^{t} \mod n$

【０１７６】４．証明データ生成装置１１中の指数生成部１３０は、ユーザ固有情報記憶部１１５に記憶されているユーザの固有情報ｅを取得し、式２１の計算を実行する。

【数２１】（２１）　　$F(n, e)$

【０１７７】５．証明データ生成装置１１中の第２演算部１１４は、指数生成部１３０で生成されたデータを用いて、式２２の計算を実行し差分情報Ｓを得る。

【数２２】（２２）　　$S = C^{F(n,e)} \mod n$

６．証明データ生成装置１１中の証明データ生成部１１６は、第１および第２演算部１１２、１１４からＲ’およびＳを得て、式２３の計算を行ないＲを得る。

【数２３】（２３）　　$R = R' S^{-1} \mod n$

ただし、S^{-1}は法ｎのもとでのＳの逆数、即ち、式２４を満たす数を表す。

【数２４】（２４）　　$S \cdot S^{-1} \mod n = 1$

【０１７８】７．証明データ生成装置１１はＲを証明データ検証装置１０の受信データ記憶部１０５に返送する。

【０１７９】８．証明データ検証装置１０では、証明データ生成装置１１から受け取った証明データの検証を行うが、その検証方法は、認証用データの一部であるＣの生成方法によって異なる。

【０１８０】Ｃが第一の実施例の方法に基づいて生成されたものであれば、その検証は第一の実施例に述べられた方法に従って行われる。

【０１８１】Ｃが第二の実施例の方法に基づいて生成されたものであれば、その検証は第二の実施例に述べられた方法に従って行われる。

［第四の実施例］

【０１８２】第四の実施例では、第一乃至第三の実施例において、証明データ生成装置がユーザのＰＣあるいはワークステーション上のプログラムと、前記ＰＣあるいはワークステーションに装着されるＩＣカード、あるいはＰＣカード（ＰＣＭＣＩＡカード）などの携帯可能な演算手段によって構成される場合について述べる。

【０１８３】第一乃至第三の実施例の証明データ生成装置１１において、ユーザ固有情報ｅは秘密情報であり、外部に漏洩しないよう注意を払わなければならない。また、ユーザ固有情報ｅを用いた計算を実行する第２演算部１１４の動作が観測されるとユーザ固有情報ｅが漏洩する危険がある。第三の実施例における関数Ｆ（ｘ，ｙ）の計算過程が観測された場合も同様である。即ち、ユーザ固有情報ｅの漏洩を防ぐためには、ユーザ固有情報記憶部１１５、第２演算部１１４及び指数生成部１３０の内部が外部から観測されることを防止しなければならない。この目的を達成するためには、証明データ生成装置１１の一部をハードウェアとして構成すると有効である。

【０１８４】このようなハードウェアとして、ＩＣカード・ＰＣカードのような携帯性のある手段を用いることにすれば、更にユーザの利便性を高めることができる。証明データ生成装置の内、ユーザに固有な部分は、ユーザ固有情報記憶部とアクセスチケット記憶部のみである。従って、例えば、ユーザ固有情報記憶部１１５と、アクセスチケット記憶部１１３と、第２演算部１１４と、指数生成部１３０とをＩＣカード・ＰＣカード中に構成し、証明データ生成装置の残りの部分をユーザが使用するＰＣあるいはワークステーション上で動作するプログラムとして構成することにすれば、証明データ生成装置１１のうち各ユーザに固有な部分は、それぞれのユーザが携帯可能なＩＣカード・ＰＣカードとして実現され、ユーザに依存しない共通部分はプログラムとして任意のＰＣあるいはワークステーションに共通に構成されることとなる。このような構成によって、どのユーザでも、自分のＩＣカード・ＰＣカードを、前記プログラムがインストールされた任意のＰＣあるいはワークステーションに装着するだけで、該ＰＣあるいはワークステーションを自分用の証明データ生成装置として利用することが可能となる。

【０１８５】さて、内部メモリーに格納されたデータやプログラムが外部から観測されたり、改竄されたりすることを防止するための特殊な構成を持つハードウェアを、耐タンパーハードウェア（タンパーレジスタントハードウェア）と呼ぶ。耐タンパーハードウェアの構成法としては、例えば、特許第１８６３９５３号、特許第１８６０４６３号、特開平３－１００７５３号公報等が知られている。

【０１８６】特許第１８６３９５３号においては、情報記憶媒体の周囲に、各種の導体パターンを持つ複数のカードからなる包囲体を設ける。検出される導体パターンが予測されるパターンと異なる時に記憶情報を破壊する。

【０１８７】特許第１８６０４６３号においては、情報記憶媒体の周囲に導体巻線を形成するとともに積分回路等からなる検知回路を設けることで、電子回路領域への侵入があった場合には電磁エネルギーの変動を検知し記憶情報を破壊する。

【０１８８】特開平３－１００７５３号公報においては、ハードウェア内部に光検知器を設け、ハードウェアに力が加えられて破壊された場合や穿孔されたときに入る外光を光検知器が検知し、記憶破壊装置が記憶情報をリセットする。

【０１８９】これらの耐タンパーハードウェアを、ＩＣカードやＰＣカード（ＰＣＭＣＩＡカード）のような携帯可能な演算装置として実現することにより、ユーザに対する更なる利便を提供することができる。

【０１９０】また、ＩＣカードに実装されるマイクロコントローラーは、高密度実装ゆえに、それ自体で相当の耐タンパー特性を有しているとされている。

【０１９１】図１７は、第一および第二の実施例において、ユーザ固有情報ｅを保持するユーザ固有情報記憶手段１１５と、差分情報を生成する第二演算手段１１４とが、ＩＣカードのような耐タンパーハードウェア１６０に封入されている構成を示している。

【０１９２】図１８は、第三の実施例において、ユーザ固有情報ｅを保持するユーザ固有情報記憶部１１５と、差分情報を生成する第２演算部１１４に加えて、指数生成部１３０も耐タンパーハードウェア１６１に封入されている構成を示している。

【０１９３】ＩＣカード側Ｉ／Ｆ部１４１は、ホストとＩＣカードの通信を司るＩＣカード側インターフェースであり、具体的には、通信用バッファと通信プログラムから構成される。証明データ生成装置の内の残りの部分は、ユーザのＰＣあるいはワークステーション上で動作するプログラムとして構成される。耐タンパーハードウェア１６１中の各手段の作用は第一乃至第三の実施例に述べた通りであるので、以下では、その部分の作用については解説しない。また、説明を簡略にする目的で耐タンパーハードウェアをＩＣカードであるものと仮定するが、この仮定はこの発明の一般性をなんら束縛するものではない。図１９は、図１７および図１８におけるデータのフローを示している。

【０１９４】つぎに、動作について説明する。

１．ユーザがアクセスすることによって、証明データ検証装置１０が起動される。

【0195】2．証明データ検証装置10は、認証用データCとアクセスチケット公開鍵記憶部101に記憶されているRSA暗号の法数nとの組を証明データ生成装置11中の受信データ記憶部111に書き込む。
【0196】3．証明データ生成装置11中のホスト側インターフェース部140は、受信データ記憶部111に書き込まれた認証用データCとnを、ICカード側インターフェース部141に引き渡す。ホスト側インターフェース部140は、ICカード中に設けられたICカード側インターフェース部141と協調して、ホスト・ICカード間のデータ通信を司る。
【0197】4．アクセスチケット検索部142は、RSA法数nを検索のキーとして、アクセスチケット記憶部113に記憶されているアクセスチケットtを検索・取得する。
【0198】5．第1演算部112は、受信データ記憶部111に書き込まれたRSA法数nのもとで式25を実行し中間情報R'を得る。
【数25】（25）　$R' = C^t \mod n$
【0199】6．次いで、ホスト側インターフェース部140は、ICカード側インターフェース部141にコマンドを発行し、その返り値として差分情報Sを得る。
【0200】アクセスチケット及びICカード中の手段が第一あるいは第二の実施例に即して構成されている場合には、差分情報Sは式26によって計算される値である。
【数26】（26）　$S = C^e \mod n$
【0201】アクセスチケット及びICカード中の手段が第三の実施例に即して構成されている場合には、差分情報Sは式27によって計算される値である。
【数27】（27）　$S = C^{F(n,e)} \mod n$
7．証明データ生成装置11中の証明データ生成部116は、第1および第2演算部112、114からR'およびSを得て、第一および第二の実施例に即している場合は式28、第三の実施例に即している場合には式29の計算を行ないRを得る。
【数28】（28）　$R = R' S \mod n$
【数29】（29）　$R = R' S^{-1} \mod n$
【0202】8．証明データ生成装置11はRを証明データ検証装置10の受信データ記憶部105に返送する。
【0203】上記の作用において、中間情報R'と差分情報Sの計算が、ユーザのPCあるいはワークステーションであるホスト側と、演算機能を内蔵するICカード側で並列に実行されるため、証明データ生成手段11が認証用データC及び法数nを受け取ってから、証明データRを計算するまでの実行時間を短縮することができ、よって処理効率を向上させている。
【0204】この実施例では、アクセスチケット記憶部113には複数のアクセスチケットが記憶されるが、アクセスチケットが異なればそのRSA法数nが異なるので、アクセスチケットは、nをキーとして検索ができるようにnと対応づけて記憶される。
【0205】また、アプリケーションやサーバがアクセス制御のために利用するRSA法数nは、アプリケーションやサーバ毎に異なるのが基本である。
【0206】アクセスチケット検索部142は、証明データ検証装置10から与えられるRSA法数nをキーとして、適切なアクセスチケットを検索し、以後の証明データの生成に供する。この検索機能により、証明データ生成装置11は、ユーザになんら負担を強いることなく、アクセスしている対象（個別のアプリケーションや個別のサーバ）に応じて適切な証明データを計算し、返送することが可能となる。
【0207】［第五の実施例］この発明における第五の実施例では、第三の実施例で用いたRSA公開鍵暗号の代わりに、Pohlig－Hellman非対称鍵暗号を用いる。
【0208】Pohlig－Hellman非対称鍵暗号は、法数として大きな素数pを用いる点で，法数として2つの素数の積n（＝pq）を用いるRSA公開鍵暗号と異なる外は、RSA公開鍵暗号と同一の暗号方式である。しかし、RSA公開鍵暗号では、一方の鍵Eと法数nから、もう一方の鍵Dを計算することが非常に困難であったため、E及びnを公開鍵として用い、Dを個人の秘密として用いることが可能であった。一方、Pohlig－Hellman非対称鍵暗号暗号では、EとpとからDが容易に計算できるため、EとpとをDを公開鍵として用いることはできない。即ち、EとDとの両方を当事者間の秘密としておく必要があり、DES（Data Encryption Standard）のような共通鍵暗号と同様の利用形態を採らざるを得ない。
【0209】この実施例では、アクセスチケットtは次の式30に基づいて生成されるデータである。
【数30】
（30）　$t = D + F(p, e)$
上式中の各記号は以下を表す。
【0210】pは十分大きな素数である。
【0211】ユーザ固有情報eはユーザ毎に異なる数であり、ユーザを識別するために用いられる。
【0212】アクセスチケット秘密鍵Dは、法数pのもとでのPohlig－Hellman暗号の鍵の一方であり、式31を満たす。
【数31】
（31）　$gcd(D, p-1) = 1$
ここで、gcd（x，y）は二数x、yの最大公約数を表す。
【0213】式31によって表現される性質は、式32を満たす数Eが存在することを保証する。
【数32】

（32）　　$ED \mod p-1 = 1$

【0214】二変数関数F（x，y）は関数値が衝突しにくい二変数関数であり、例えば、前述の一方向ハッシュ関数hを利用して、式33のように定めることができる。

【数33】

（33）　　$F(x, y)=h(x \mid y)$

つぎに、図20および図21を参照して第五の実施例についてさらに詳細に説明する。図20は第五の実施例の構成を示し、図21は図20におけるデータのフローを示している。図20において、証明データ検証装置20は、鍵記憶部401、乱数発生部402、乱数記憶部403、受信データ記憶部405、乱数化部421、認証用素データ記憶部422、乱数効果除去部423および実行手段310を含んで構成されている。また、証明データ生成部41は、受信データ記憶部411、第1演算部412、アクセスチケット記憶部413、第2演算部414、ユーザ固有情報記憶部415、証明データ生成部416、および指数生成部430を含んで構成されている。

【0215】つぎに、動作について説明する。

1．ユーザがアクセスすることによって、証明データ検証装置40が起動される。

【0216】2．証明データ検証装置40は、認証用データCと鍵記憶部401に記憶されている法数pとの組を証明データ生成装置41中の受信データ記憶部411に書き込む。

【0217】この実施例では、Cの生成方法としては、第二の実施例で述べた方法に準じた方法によるものとするが、第一の実施例で述べた方法に準じた方法を構成することも難しくない。

【0218】証明データ検証装置中40の乱数発生部402によって、乱数rを鍵記憶部401に保持されている法数pと互いに素になるように生成し、乱数記憶部403に記録する。乱数化部421は、鍵記憶部401に格納されてい指数Eと法数pを取得し、さらに認証用素データ記憶部422に記憶されているデータC'を取得して、式34の計算を行なう。

【数34】（34）　　$C=r^{E}C' \mod p$

ここで、認証用素データC'はデータKに対して関係式35を満たすように生成され、認証用素データ記憶部305に格納された値である。

【数35】（35）　　$C'=K^{E} \mod p$

【0219】3．証明データ生成装置41中の第1演算部412は、アクセスチケット記憶部413に記憶されているアクセスチケットtを取得し、受信データ記憶部411に書き込まれたRSA法数pのもとで式36を実行し中間情報R'を得る。

【数36】（36）　　$R'=C^{t} \mod p$

【0220】4．証明データ生成装置41中の指数生成部430は、ユーザ固有情報記憶部415に記憶されているユーザの固有情報eを取得し、式37の計算を実行する。

【数37】（37）　　$F(p, e)$

【0221】5．証明データ生成装置11中の第2演算部414は、指数生成部430で生成されたデータを用いて、式38の計算を実行し差分情報Sを得る。

【数38】（38）　　$S=C^{F(p,e)} \mod p$

6．証明データ生成装置41中の証明データ生成部416は、第1および第2演算部412、414からR'およびSを得て、式39の計算を行ないRを得る。

【数39】（39）　　$R=R' S^{-1} \mod p$

ただし、S^{-1}は法pのもとでのSの逆数、即ち、式40を満たす数を表す。

【数40】（40）　　$SS^{-1} \mod p = 1$

【0222】7．証明データ生成装置41はRを証明データ検証装置40の受信データ記憶部405に返送する。

【0223】8．証明データ検証装置10中の乱数効果除去部423は、乱数記憶部403中から先に生成した乱数rを取り出し、式41の計算を行なう。

【数41】（41）　　$K'=r^{-1}R \mod p$

証明データ生成装置41において用いられるアクセスチケットtとユーザの第一の固有情報eの組合せが正しい場合に限り、計算の結果得られたK'とKが一致することに注意せよ。

［第六の実施例］

【0224】この発明の第六の実施例では、第三の実施例におけるRSA公開鍵暗号の代わりに、ElGamal公開鍵暗号を用いた構成例を示す。

【0225】この発明における第六の実施例では、アクセスチケットtは次の式42に基づいて生成されるデータである。

【数42】

（42）　　$t = X+F(p, e)$

上式中の各記号は以下を表す。

【0226】pは十分大きな素数である。

【0227】ユーザ固有情報eはユーザ毎に異なる数であり、ユーザを識別するために用いられる。

【0228】アクセスチケット秘密鍵Xは、法数pのもとでのElGamal暗号の秘密鍵であり、Yを対応する公開鍵であるとする。即ち、式43を満たす。

【数43】（43）　　$Y = a^{X} \mod p$

ここで、aは位数pの有限体の乗法群の生成元、即ち、式44及び45を満たす。

【数44】（44）　　$a \neq 0$

【数45】

（45）　　$\min\{x>0 \mid a^{x}=1 \mod p\} = p-1$

また、Yをアクセスチケット公開鍵と呼ぶ。

【0229】二変数関数F（x，y）は関数値が衝突しにくい二変数関数であり、例えば、前述の一方向ハッシュ関数hを利用して、式46のように定めることができる。

【数46】

（46）　　F（x，y）＝h（x｜y）

つぎに、図22および図23を参照して第六の実施例をさらに説明する。図22は第六の実施例の構成を示し、図23は第六の実施例におけるデータのフローを示している。図22において、証明データ検証装置50は、アクセスチケット公開鍵記憶部501、乱数発生部502、乱数記憶部503、受信データ記憶部505、乱数化部521、認証用素データ記憶部522、乱数効果除去部523および実行手段310を含んで構成されている。証明データ生成部51は、受信データ記憶部511、第1演算部512、アクセスチケット記憶部513、第2演算部514、ユーザ固有情報記憶部515、証明データ生成部516、および指数生成部530を含んで構成されている。

【0230】つぎに動作について説明する。

1．ユーザがアクセスすることによって、証明データ検証装置50が起動される。

【0231】2．証明データ検証装置50は、認証用データの組u、Cと、アクセスチケット公開鍵記憶部501に記憶されている法数pとを、証明データ生成装置51中の受信データ記憶部511に書き込む。

【0232】認証用素データ記憶部522には、認証用素データとしてu，C'が記憶されているが、それらは次の性質を満たす。

【0233】uは、上記aを法pのもとで適当な乱数zを指数としてべき乗した数であり、即ち、式47を満たす。

【数47】（47）　　$u = a^z \mod p$

【0234】C'は、アクセスチケット公開鍵Yを、法pのもとで、上記乱数zを指数としてべき乗した数と、適当なデータKとの積であり、式48を満たす。

【数48】（48）　　$C' = Y^z K \mod p$

【0235】認証用データCは、次のように生成される。

【0236】証明データ検証装置50は、乱数発生部502によって、乱数rをアクセスチケット公開鍵記憶部501に保持されている法数pと互いに素になるように生成し、乱数記憶部503に記録する。

【0237】次いで、乱数化部521は、認証用素データ記憶部522に記憶されているデータC'を取得して、式49の計算を行なう。

【数49】（49）　　$C = rC' \mod p$

【0238】3．証明データ生成装置51中の第1演算部512は、アクセスチケット記憶部513に記憶されているアクセスチケットtを取得し、受信データ記憶部511に書き込まれた法数pのもとで式50を実行し中間情報Sを得る。

【数50】（50）　　$S = u^t \mod p$

【0239】4．証明データ生成装置51中の指数生成部530は、ユーザ固有情報記憶部515に記憶されているユーザの固有情報eを取得し、式51の計算を実行する。

【数51】

（51）　　F（p，e）

【0240】5．証明データ生成装置51中の第2演算部514は、指数生成部530で生成されたデータを用いて、式52の計算を実行し差分情報S'を得る。

【数52】

（52）　　$S' = u^{F(p,e)} \mod p$

【0241】6．証明データ生成装置51中の証明データ生成部516は、第1および第2演算部512、514からSおよびS'を得て、式53の計算を行ないRを得る。

【数53】

（53）　　$R = S^{-1}S'C \mod p$

ただし、S^{-1}は法pのもとでのSの逆数、即ち、式54を満たす数を表す。

【数54】（54）　　$SS^{-1} \mod p = 1$

【0242】7．証明データ生成装置51はRを証明データ検証装置50の受信データ記憶部505に返送する。

【0243】8．証明データ検証装置10中の乱数効果除去部523は、乱数記憶部503中から先に生成した乱数rを取り出し、式55の計算を行なう。

【数55】（55）　　$K' = r^{-1}R \mod p$

証明データ生成装置51において用いられるアクセスチケットtとユーザの固有情報eの組合せが正しい場合に限り、計算の結果得られたK'とKが一致することに注意せよ。さて、上記の形態を直接実施した場合、次のような問題が生じる。即ち、同一の認証用素データu，C'を、複数回のアクセス資格認証手続きに適用することにより、ユーザ固有情報やアクセスチケットなしに証明データ生成装置11の作用を模倣する装置を構成することが可能となる。まず、初回の認証手続きにおいて、証明データ検証装置10から発行される認証用素データCと証明データ生成装置11が生成する証明データRから、$H = RC^{-1} \mod p$を計算する。模倣装置には、ユーザ固有情報及びアクセスチケットの代わりにこのHを記録しておく。証明データ検証装置10が発行する任意の認証用素データ（u，C）に対し、模倣装置が式$R = HC \mod p$に従って証明データRを生成し、証明データ検証装置10に返すようにすればよい。この攻撃に対処する方法として、認証用素データ記憶部522に認証用素データの組u，C'を必要な数だけ記

憶しておいて、認証手続きの都度使い捨てにする方法が考えられる。ここで、相異なる認証用素データでは、その生成のために用いられる乱数ｚが互いに相違するようにする。ｕは、$u=a^k \mod p$で定義されるが、ｋは乱数であったことに留意されたい。

［第七の実施例］

【０２４４】この発明の第七の実施例においては、アクセス資格認証の特徴情報としてＥｌＧａｍａｌ署名の署名鍵を用いる構成例を述べる。

【０２４５】この発明における第七の実施例では、アクセスチケットｔは式５６に基づいて生成されるデータである。

【数５６】

（56）　$t = X+F(p, e)$

また、Ｙをアクセスチケット公開鍵と呼ぶ。

【０２４９】二変数関数Ｆ（ｘ，ｙ）は関数値が衝突しにくい二変数関数であり、例えば、前述の一方向ハッシュ関数ｈを利用して、式６０のように定めることができる。

【数６０】

（60）　$F(x, y)=h(x \mid y)$

【０２５０】つぎに図２４および図２５を参照してさらに第七の実施例について説明する。図２４は第七の実施例の構成を示し、図２５は第七の実施例におけるデータのフローを示している。図２４において、証明データ検証装置６０は、アクセスチケット公開鍵記憶部６０１、乱数発生部６０２、乱数記憶部６０３、受信データ記憶部６０５、検証部６０６、実行部６０７およびエラー処理部６０８を含んで構成されている。また、証明データ生成装置６１は、受信データ記憶部６１１、乱数発生部６１２、第１演算部６１３、第２演算部６１４、アクセスチケット記憶部６１５、およびユーザ固有情報記憶部６１６を含んで構成されている。つぎに動作について説明する。

１．ユーザがアクセスすることによって、証明データ検証装置６０が起動される。

【０２５１】２．証明データ検証装置６０は、認証用データＣと、アクセスチケット公開鍵記憶部６０１に記憶

（59）　$\min\{x>0 \mid a^x=1 \mod p\} = p-1$

されている法数ｐと、生成元ａとを、証明データ生成装置６１中の受信データ記憶部６１１に書き込む。認証用データＣは、次のように生成される。

【０２５２】証明データ検証装置６０は、乱数発生部６０２によって、乱数ｒをアクセスチケット公開鍵記憶部６０１に保持されている法数ｐと互いに素になるように生成し、前記ｒを乱数記憶部６０３に記録するとともに、認証用データＣとする（Ｃ＝ｒ）。

【０２５３】３．証明データ生成装置６１中の乱数生成部６１２は、法数ｐ－１と互いに素であるような乱数ｋを生成する。

【０２５４】第１演算部６１３は、前記乱数ｋと、受信データ記憶部６１１に書き込まれた法数ｐと、生成元ａとから、第一の証明データＲを式６１に従って計算する。

【数６１】（61）　$R = a^k \mod p$

【０２５５】第２演算部６１４は、アクセスチケット記憶部６１５に記憶されているアクセスチケットｔと、ユーザ固有情報記憶部６１６に記憶されているユーザ固有情報ｅと、前記乱数ｋと、前記第一の証明データＲと、受信データ記憶部６１１に書き込まれた認証用データＣと、法数ｐとから、第二の証明データＳを式６２に従って計算する。

【数６２】

（62）　$S = (C-R(t-F(p, e)))k^{-1} \mod p-1$

【０２５６】４．証明データ生成装置６１は第一および第二の証明データであるＲ及びＳを証明データ検証装置６０の受信データ記憶部６０５に返送する。

【０２５７】５．証明データ検証装置６０中の検証部６０６は、乱数記憶部６０３に記憶されている乱数ｒ（＝Ｃ）と、アクセスチケット公開鍵記憶部６０１に記憶されているＹ及びｐとを取り出し、式６３によって、証明データＲ及びＳを検証する。

【数６３】（63）　$a^r = Y^R R^S \mod p$

上式中の各記号は以下を表す。

【０２４６】ｐは十分大きな素数である。

【０２４７】ユーザ固有情報ｅはユーザ毎に異なる数であり、ユーザを識別するために用いられる。

【０２４８】アクセスチケット秘密鍵Ｘは、法数ｐのもとでのＥｌＧａｍａｌ署名の署名鍵であり、Ｙを対応する公開鍵であるとする。即ち、式５７を満たす。

【数５７】

（57）　$Y = a^X \mod p$

ここで、ａは位数ｐの有限体の乗法群の生成元、即ち、式５８及び５９を満たす。

【数５８】（58）　$a \neq 0$

【数５９】

［第八の実施例］

【０２５８】この発明の第八の実施例では、アクセスチケットの生成方法について述べる。

【０２５９】第一乃至第七の実施例におけるアクセスチケットの生成には、秘密数に基づく計算が必要である。従って、アクセスチケットの生成は、計算に用いる秘密数が漏洩したり、計算の中間結果が露呈する心配のない安全な装置で実行される必要がある。

【０２６０】このような安全な装置を構成するための最も容易な方法は、アクセスチケット発行サービスをユーザに提供するサーバを、ユーザが使用するＰＣあるいは

ワークステーションから独立な計算機上に構築することである。サーバは、ユーザからの要求に応じてアクセスチケットを生成する。サーバの構成に当たっては、外部からの侵入を遮断するように構成することにより、秘密数およびアクセスチケットの計算手順を守る。

【０２６１】例えば、アクセスチケット発行サーバを、施錠され、出入りが厳重に管理される個室内の計算機上に構成することにより、外部からの侵入を遮断することが可能となる。

【０２６２】また、ユーザの利便を向上させるために、前記アクセスチケット発行サーバをネットワークに接続し、ユーザからのアクセスチケット発行要求をネットワークを介して受け取り、生成したアクセスチケットをやはりネットワークを介してユーザに配送するように構成することも可能である。

【０２６３】このように、アクセスチケット発行サーバをネットワークに接続する場合には、ファイアウォール技術（D. Brent Chapman & Elizabeth D. Zwicky, Building Internet Firewalls, O'Reilly & Associates, Inc.あるいは邦訳、ファイアウォール構築、オライリー・ジャパンを参照）を利用して、ネットワークを介した外部からの侵入に対しても十分に安全性が保たれるよう構築される必要がある。

【０２６４】第一乃至第七の実施例におけるアクセスチケットは、その正当な使用者（アクセスチケットを計算する際に用いたユーザ固有情報ｅを保持するユーザ）以外には利用できない形式で生成されている。

【０２６５】第一乃至第七の実施例におけるアクセスチケットは、更に厳密な安全基準のもとに生成されてい

$$1 \leqq d_U \leqq (p_U - 1)(q_U - 1)$$
$$1 \leqq e_U \leqq (p_U - 1)(q_U - 1) \quad (64)$$
$$e_U d_U \equiv 1 \mod (p_U - 1)(q_U - 1)$$

ここで、n_Uは全てのユーザに共有される定数N以上であるという条件を付け加える。

【０２７０】ユーザUへのアクセスチケットは以下のように構成される。

【０２７１】ＲＳＡ公開鍵ペアの公開鍵（Ｅ，ｎ）をアクセスチケットの公開鍵とし、該公開鍵と対をなす秘密鍵をＤとする。ｎの素因数分解をｎ＝ｐｑとする時、関係式６５が成り立つ。

【数６５】

$$1 \leqq D < N \quad (65)$$
$$DE \equiv 1 \mod (p-1)(q-1)$$

アクセスチケットt_Uは式６６で定義される

【数６６】

$$t_U = D^{e_U} \mod n_U \quad (66)$$

【０２７２】この実施例におけるアクセス資格認証の特徴情報は、前記ＲＳＡ公開鍵ペアの個人鍵Ｄである。

【０２７３】第一乃至第七の実施例の場合と同様、この実施例における証明データ生成装置１１は、アクセス資格認証の特徴情報を知りえること、即ち、与えられた認証用データに対応して、正しい証明データを計算し得ることを、証明データ検証装置１０との通信を介して証明する。

【０２７４】この実施例の特徴は、アクセス資格認証の特徴情報であるＤを暗号化して得られるデータがアクセスチケットであり、ユーザの固有情報がこの暗号化を解くための唯一の復号鍵である点にある。更にいえば、ユーザの固有情報をＲＳＡ公開鍵暗号の個人鍵としている所から、対応する公開鍵を知りえる何人でもアクセスチケットを生成しえる点にある。以下に、本実施例における作用を図２６を参照して述べる。

【０２７５】１．証明データ検証装置１０は、認証用データＣを証明データ生成装置１０の受信データ記憶部７１１に書き込む。

る。即ち、不正なアクセスを試みるユーザが、本人向けあるいは他人向けを問わず、任意個数のアクセスチケットを集めたとしても、そこから、別のアクセスチケットを偽造したり、第一乃至第五の実施例で述べた証明データ生成装置の動作を模倣する装置を構成することは不可能である。

【０２６６】上記のようなアクセスチケットの安全性から、アクセスチケット発行サーバが生成したアクセスチケットを、電子メールのような比較的安全性の低い配送手段を利用してユーザに配送することも可能となる。

［第九の実施例］

【０２６７】この実施例では、第一乃至第七の実施例とは異なるユーザの固有情報およびアクセスチケットの構成法を述べる。この構成方法の特徴は、アクセスチケットの生成に秘密情報を必要としない点にある。

【０２６８】従って、アクセスチケット生成に際して、第八の実施例で述べたような、外部からの侵入に対して安全に構築されたアクセスチケット発行サーバは必要ない。ユーザは、所有するＰＣあるいはワークステーション上で動作するプログラムによって自由にアクセスチケットを生成することができる。プログラム中には、秘密の定数や秘密の手続きは存在せず、プログラムを解析したとしても不正アクセスを可能とするいかなる情報も取り出すことはできない。

【０２６９】ユーザUの固有情報はＲＳＡ公開鍵ペアの個人鍵ｄである。このユーザの固有情報に対応する公開鍵を（e_U，n_U）とする。即ち、異なる２つの大きい素数p_Uとq_Uに対し$n_U = p_U q_U$であり、d_U及びe_Uは関係式６４を満たすように決定された整数である。

【数６４】

【0276】2．証明データ生成装置11の復号鍵生成部712は、ユーザ固有情報記憶部715中に記憶されたユーザの固有情報d_Uと、アクセスチケット記憶部713中に記憶されたアクセスチケットt_Uを取得し、式67に基づきD'を計算する。

【数67】（67）　　$D' = t_U^{d_U} \bmod n_U$

3．証明データ生成部714は、復号鍵生成部712によって生成された前記D'と、受信データ記憶部711に記憶されている認証用データCを入力として式68の計算を行ない、Rを求める。証明データ生成部714は、計算結果を返信データとして証明データ検証装置に送信する。

【数68】（68）　　$R = C^{D'} \bmod n$

【0277】4．証明データ検証装置は、証明データRの正当性を検証する。

【0278】アクセスチケット$t_U = D^{e_U} \bmod n_U$におけるアクセスチケットの秘密鍵Dは、ユーザUに対しても秘密に保たれなければならないので、上記証明データ生成装置11の装置構成のうち、ユーザ固有情報記憶部713、復号鍵生成部712および証明データ生成部714は耐タンパー特性を有する防御手段760中に封入される。

【0279】第1乃至第七の実施例の場合と同様、証明データ生成装置11によってユーザの第一の固有情報とアクセスチケットの正しい組合せが用いられた場合に限り、証明データ生成装置によって生成される証明データRは、証明データ検証装置によって正しく検証される。

【0280】［第十の実施例］この発明の第十の実施例は、証明データ生成装置における証明データの計算に公開鍵暗号（RSA暗号）の代わりに対称鍵暗号が利用され、アクセスチケットが、前記対称鍵暗号の復号鍵（暗号化鍵と同一）Dをユーザ固有情報であるRSA公開鍵ペアの個人鍵に対応する公開鍵（e_U，n_U）で暗号化して得られるデータである点を除いては、第九の実施例とほぼ同じである。

【0281】即ち、対称鍵暗号の暗号化関数をEncrypt（鍵，平文）（出力は暗号文）、復号関数をDecrypt（鍵，暗号文）（出力は平文）と表す時、プロテクトされた証明データCは式69で定義される。

【数69】

（69）　　C＝Encrypt（D，K）

更に、アクセスチケットtUは式70で定義される

【数70】（70）　　$t_U = D^{e_U} \bmod n_U$

以下、証明データ生成装置の装置構成および作用を図26に基づいて説明する。

【0282】1．証明データ検証装置10は、認証用データCを証明データ生成装置10の受信データ記憶部711に書き込む。

【0283】2．証明データ生成装置11の復号鍵生成部712は、ユーザ固有情報記憶部715中に記憶されたユーザの固有情報d_Uと、アクセスチケット記憶部713中に記憶されたアクセスチケットt_Uを取得し、式71によりD'を計算する。計算結果は証明データ生成部714に出力される。

【数71】（71）　　$D' = t_U^{d_U} \bmod n_U$

【0311】3．証明データ生成部714は、復号鍵生成部712から得たD'と、受信データ記憶部711に記憶されている認証用データCを入力として式72の計算を行ない、Rを求める。計算結果は、返信データとして証明データ検証装置10に送信される。

【数72】

（72）　　R＝Decrypt（D'，C）

【0284】4．証明データ検証装置11中はRの検証を行い、正規の処理を続行するか、エラー処理を実行するかを決定する。

［実施例の効果］以上の説明から明らかなように、ユーザのPCあるいはワークステーション上で実行されるアプリケーションプログラムへのアクセス制御（実行制御）を目的として、上記の実施例を実施した場合、次に述べる効果を提供することができる。

【0285】1．ユーザはユーザ固有情報を固有にただ一つ保持すればよい。

【0286】2．アプリケーション作成時にはユーザ固有情報と無関係な方法でプログラムに保護処理を施す。

【0287】3．アプリケーションの実行を許可されたユーザにはアクセスチケットが発行され、該ユーザは自らのユーザ固有情報とアクセスチケットを保持することによってのみアプリケーションの実行が可能となる。

【0288】4．アクセスチケットは、正規の持ち主ではないユーザがそれを保持していたとしても、それによってアプリケーションの実行が可能ならないような方法で、安全に生成される。

【0289】これらの特徴により、ユーザ固有情報を内蔵したハードウェアをユーザに配布する場合でも、配布は各ユーザ毎に一回で済み、また、プログラム作成者は、作成する所のプログラムがだれによって利用されるかに関わりなく、一つのアプリケーションの保護処理を一通りの方法で行なえばよいこととなる。従って、従来技術の問題点であった、

◎ユーザ毎に異なるユーザ固有情報を識別するように、プログラムの保護方法をユーザ毎に変えなければならない、

◎ユーザ固有情報をアプリケーション毎に設定し、そのためアプリケーション毎にハードウェアをユーザに郵送しなければならない、

といった問題点が解決され、コストの低減と利便性の向上に大幅に寄与する。

【0290】上述の実施例によれば、アプリケーションプログラムの実行にはアクセスチケットが必要となるが、アクセスチケットは正規のユーザにのみ利用可能な

安全なディジタル情報であるため、ネットワーク等を介して簡便にユーザに配送することが出来る。

【0291】また、ユーザは利用するアプリケーションプログラムを変更する度にアクセスチケットを取り替える必要があるが、前述のようにアクセスチケットはディジタル情報であるため取り替え操作は計算機中のプログラムによって容易に行なうことができる。即ち、アプリケーションプログラムを変更する度にユーザがハードウェアを取り替えなければならないといった従来の煩雑さが解消される。

【0292】更に、上述実施例では、異なる証明データに基づく証明データ検証装置（プロシージャ）を、アプリケーションプログラム中の任意の位置に自由に配置することが可能であるため、

◎アプリケーションプログラムの部分毎に異なる実行権を設定する

◎特定の組合せのアクセスチケットを全て保持している時に限り実行権を与える

といった、きめの細かいアクセス制御を実行制御によって実現することが出来る。

【0293】なおこの発明はプログラムの実行制御に限定されるものではなく、メールのプライバシー保護やファイルおよび計算機資源へのアクセス制御にこの発明を適用することができることは明らかである。すなわちファイルやメールや計算機資源を管理する機構にこの発明の認証技術を適用すれば、ファイル等のアクセスを制御することができる。

【0294】

【発明の効果】以上説明したように、この発明によれば、証明用補助データ（アクセスチケット）を導入することにより、アクセス資格認証の特徴情報とユーザ固有情報とを独立させることができ、従って、プロテクト側も、ユーザ側も１つの固有情報を準備しておけば済む。アクセスチケットは、特定のユーザ固有情報とアクセス資格認証の特徴情報とに基づいて計算されるデータであり、またユーザ固有情報を知らずにアクセスチケットからアクセス資格認証の特徴情報を計算することは少なくとも計算量的に不可能である。そしてユーザ固有情報とアクセスチケットとの正しい組合せ、即ち、ユーザ固有情報と該ユーザ固有情報に基づいて計算されたアクセスチケットの組合せが入力された場合に限って、正しい証明用データがを計算される。従って、ユーザはあらかじめユーザ固有情報を所持し、プログラム作成者等のプロテクト者はユーザが所持するユーザ固有情報とは独立にアクセス資格認証の特徴情報を用意し、アクセスチケットをユーザの固有情報とアプリケーションプログラムの作成等に使用したアクセス資格認証の特徴情報とに応じて作成し、配布することにより、実行制御等のユーザのアクセス資格の認証を行なうことができる。

【図面の簡単な説明】

【図１】　この発明の原理的な構成例を示すブロック図である。

【図２】　この発明の第一の実施例の構成を示すブロック図である。

【図３】　第一の実施例の証明データ検証装置及び証明データ生成装置の構成を示すブロック図である。

【図４】　第一の実施例の動作を説明するフロー図である。

【図５】　第二の実施例の証明データ検証装置及び証明データ生成装置の構成を示すブロック図である。

【図６】　第二の実施例の証明データ検証装置の動作を説明するフロー図である。

【図７】　第二の実施例の証明データ検証装置の実行部の構成例を示すブロック図である。

【図８】　図７の実行部の構成例の動作を説明するフロー図である。

【図９】　第二の実施例の証明データ検証装置の実行部の他の構成例を示すブロック図である。

【図１０】　図９の実行部の構成例の動作を説明するフロー図である。

【図１１】　第二の実施例の証明データ検証装置の実行部の他の構成例を示すブロック図である。

【図１２】　図１１の実行部の構成例の動作を説明するフロー図である。

【図１３】　第二の実施例の証明データ検証装置の実行部の他の構成例を示すブロック図である。

【図１４】　図１３の実行部の構成例の動作を説明するフロー図である。

【図１５】　この発明の第三の実施例の証明データ生成装置の構成を示すブロック図である。

【図１６】　第三の実施例の証明データ生成装置の動作を説明するフロー図である。

【図１７】　この発明の第四の実施例の構成例を示すブロック図である。

【図１８】　この発明の第四の実施例の他の構成例を示すブロック図である。

【図１９】　図１７の動作を説明するフロー図である。

【図２０】　この発明の第五の実施例の構成を示すブロック図である。

【図２１】　第五の実施例のデータ検証装置の動作を説明するフロー図である。

【図２２】　この発明の第六の実施例の構成を示すブロック図である。

【図２３】　第六の実施例の動作を説明するフロー図である。

【図２４】　この発明の第七の実施例の構成を示すブロック図である。

【図２５】　第七の実施例の動作を説明するフロー図である。認証プロトコルを説明する図である。

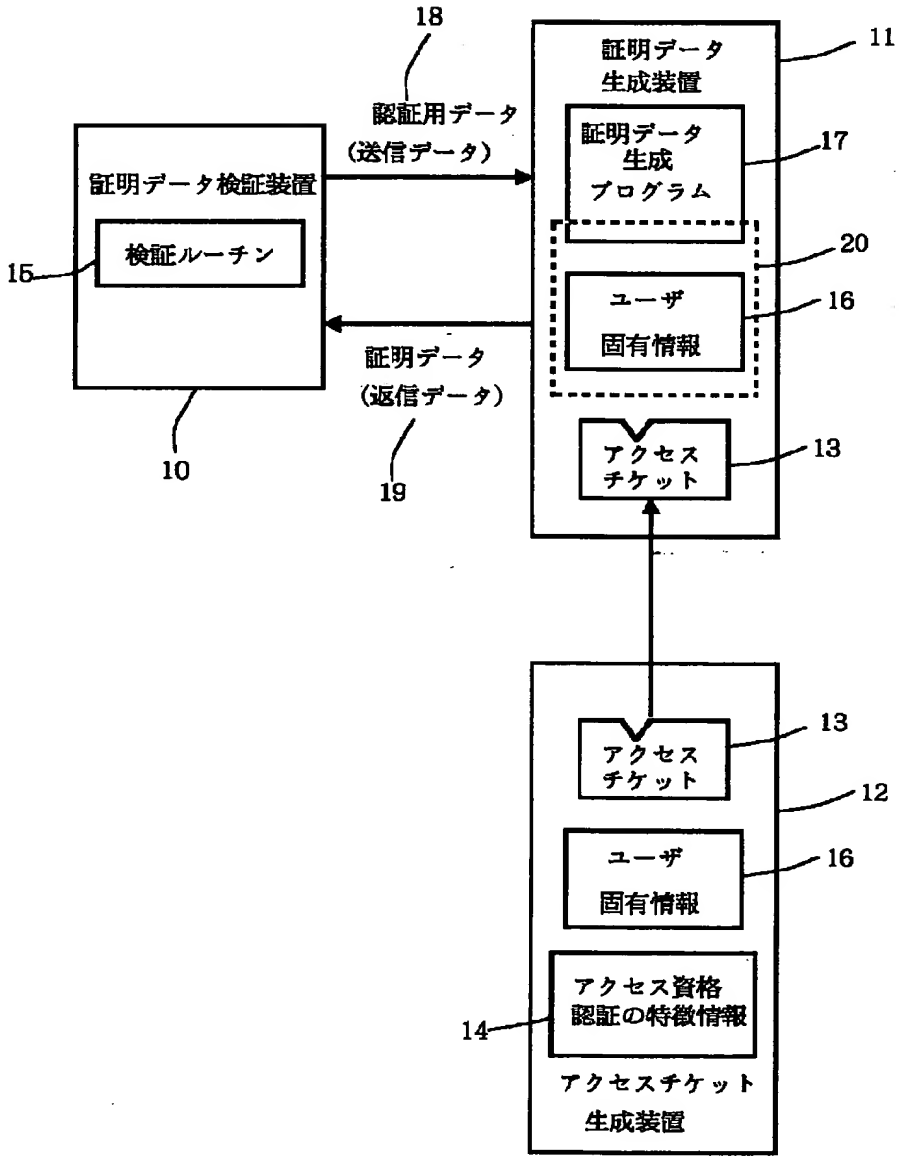
【図２６】　第九の実施例および第十の実施例のアクセ

スチケットを用いた認証を説明するブロック図である。

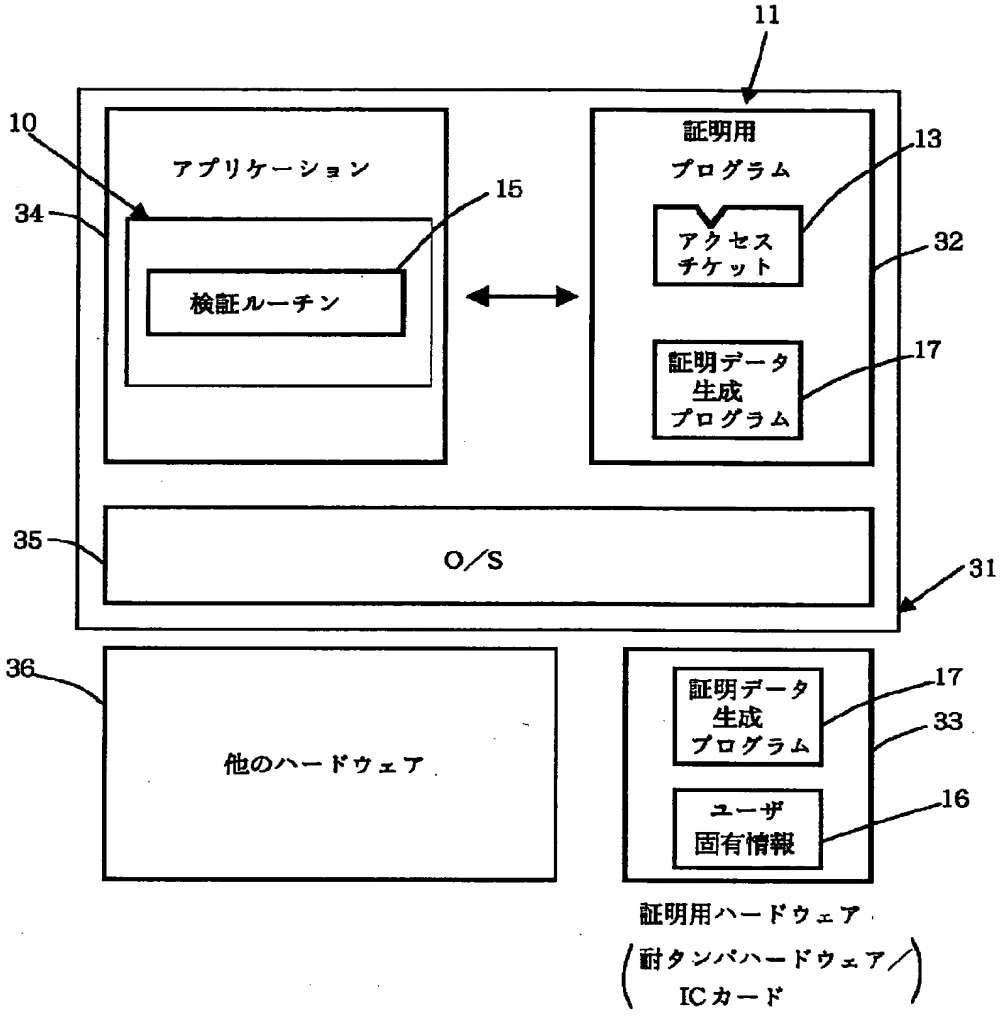
【符号の説明】

10　証明データ検証装置
11　証明データ生成装置
12　アクセスチケット生成装置
13　アクセスチケット
14　アクセス資格認証の特徴情報
15　検証ルーチン
16　ユーザ固有情報
17　証明データ生成プログラム
20　トークン（防護手段）
101　アクセスチケット公開鍵記憶部101
102　乱数発生部
103　乱数記憶部
105　受信データ記憶部
106　検証部
107　実行部
108　エラー処理部
111　受信データ記憶部
112　第1演算部
113　アクセスチケット記憶部
114　第2演算部
115　ユーザ固有情報記憶部
116　証明データ生成部

【図1】

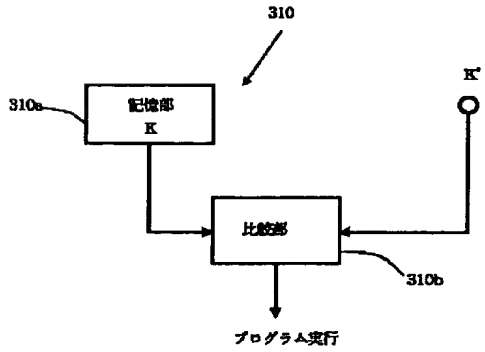


【図2】

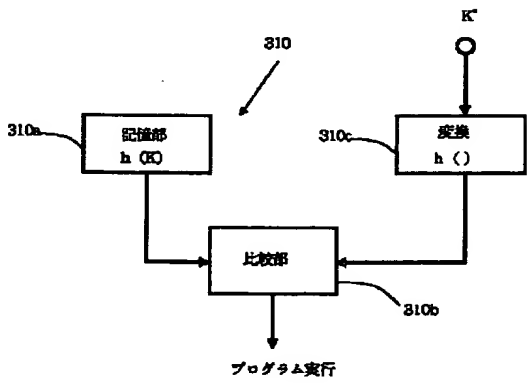


実施例の実現態様

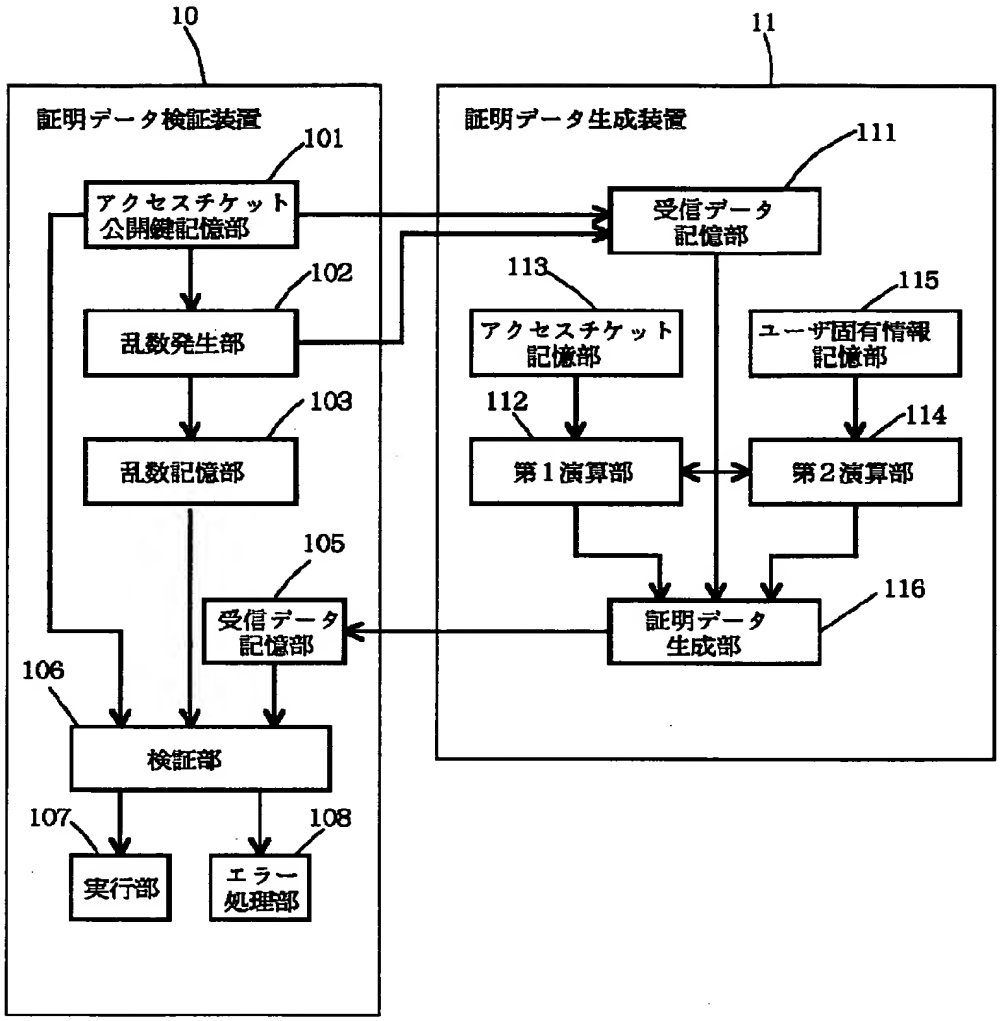
【図7】



【図9】

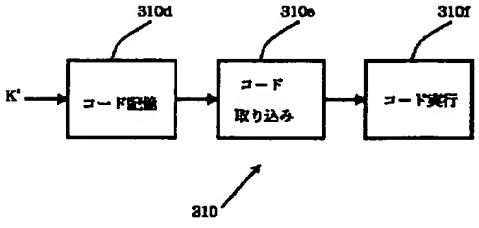


【図３】

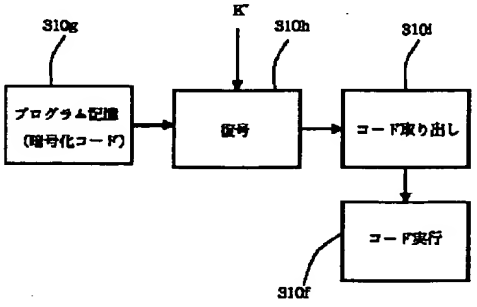


第一の実施例

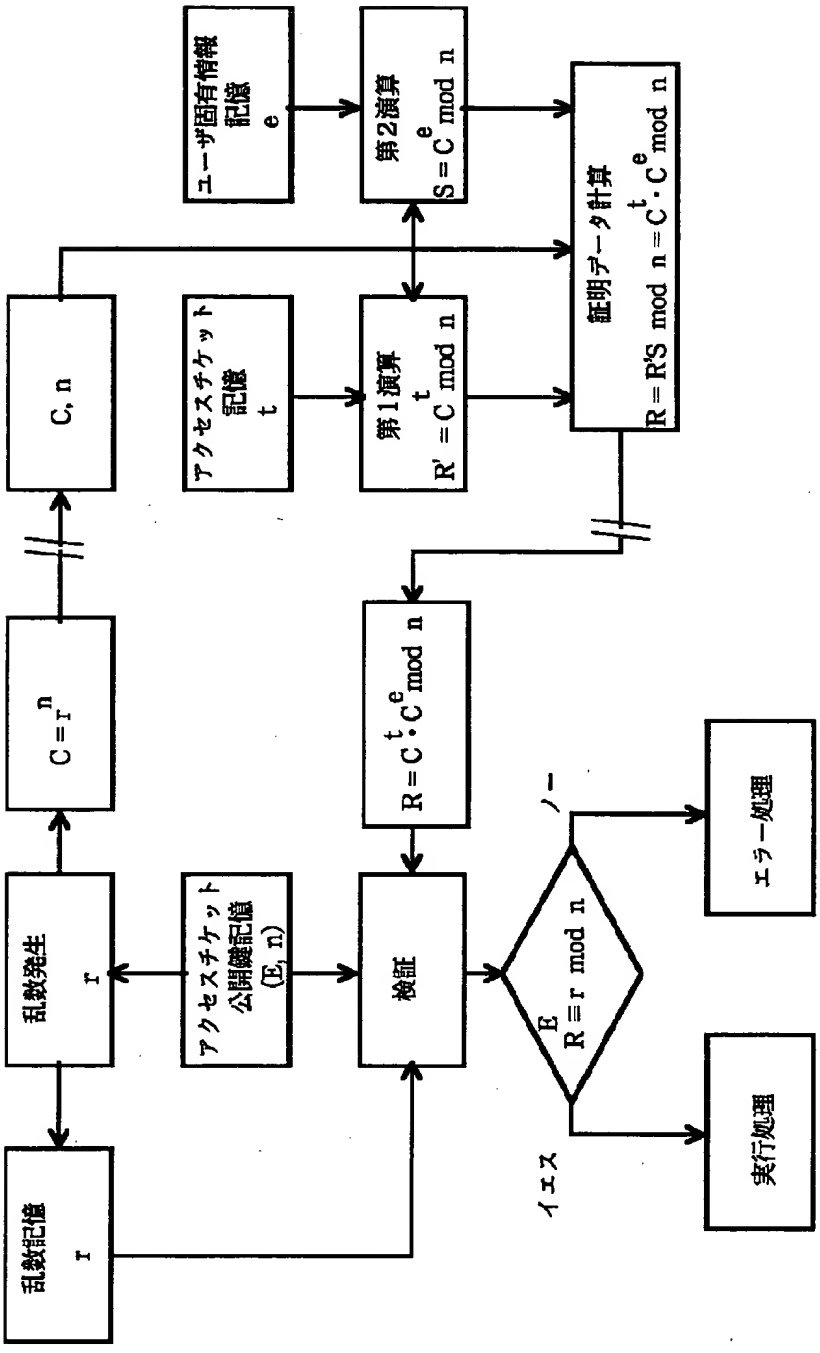
【図１１】



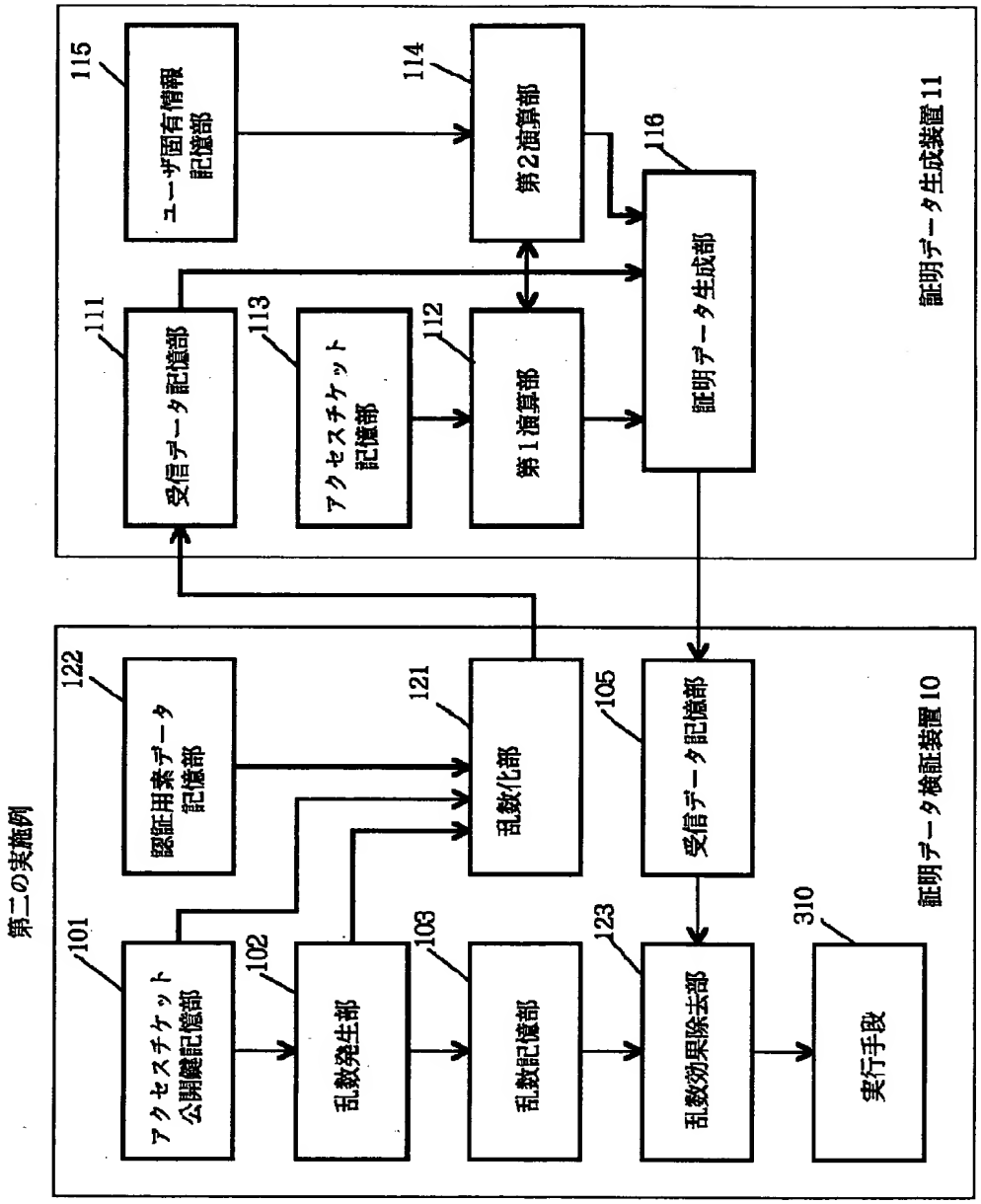
【図１３】



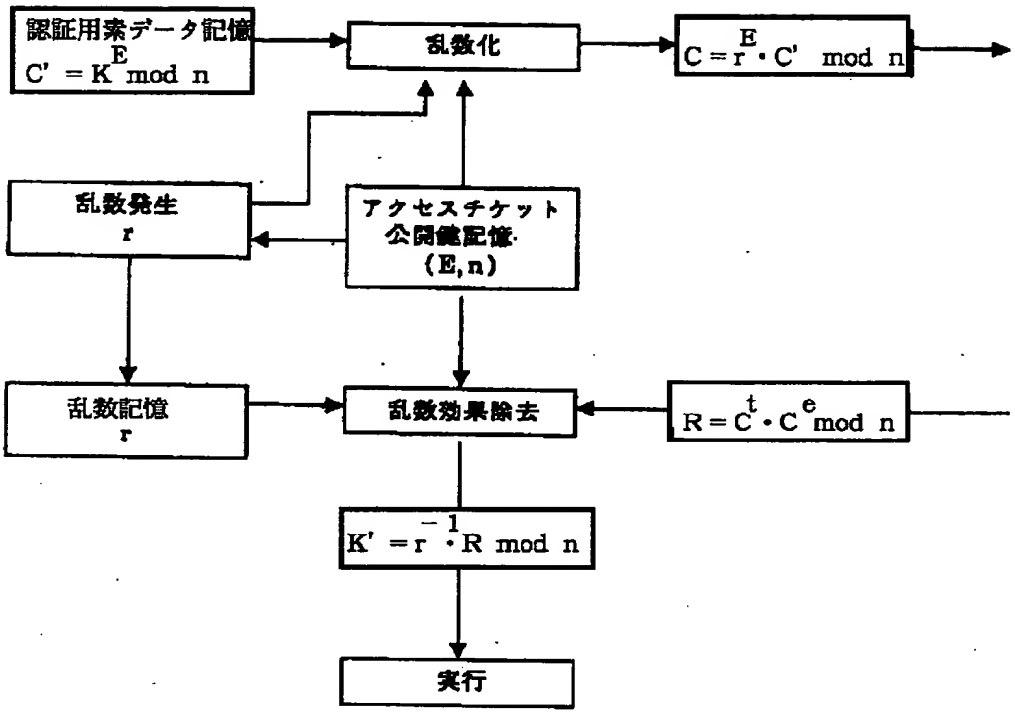
【図4】


ユーザ固有情報
記憶
e
第2演算
S＝C^e mod n
証明データ計算
R＝R'S mod n＝C^t・C^e mod n
C, n
アクセスチケット
記憶
t
第1演算
t
R'＝C mod n
C＝r^n
R＝C^t・C^e mod n
乱数発生
r
アクセスチケット
公開鍵記憶
(E, n)
検証
E
R≡r mod n
ノー
エラー処理
イエス
実行処理
乱数記憶
r

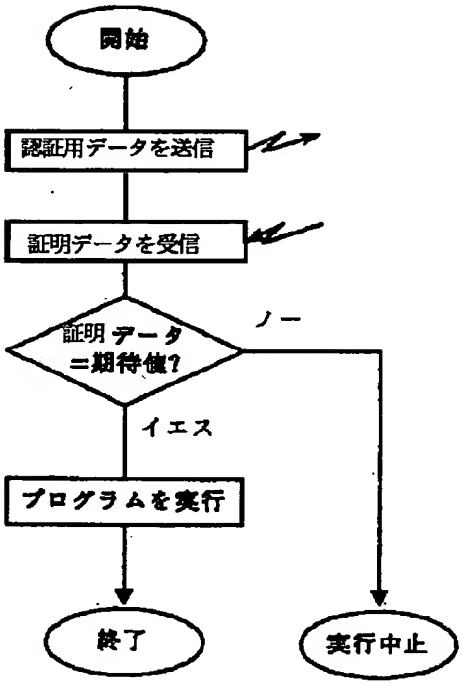
【図5】


第二の実施例
証明データ検証装置10
証明データ生成装置11
101
アクセスチケット公開鍵記憶部
102
乱数発生部
103
乱数記憶部
105
受信データ記憶部
111
受信データ記憶部
112
第1演算部
113
アクセスチケット記憶部
114
第2演算部
115
ユーザ固有情報記憶部
116
証明データ生成部
121
乱数化部
122
認証用乗データ記憶部
123
乱数効果除去部
310
実行手段

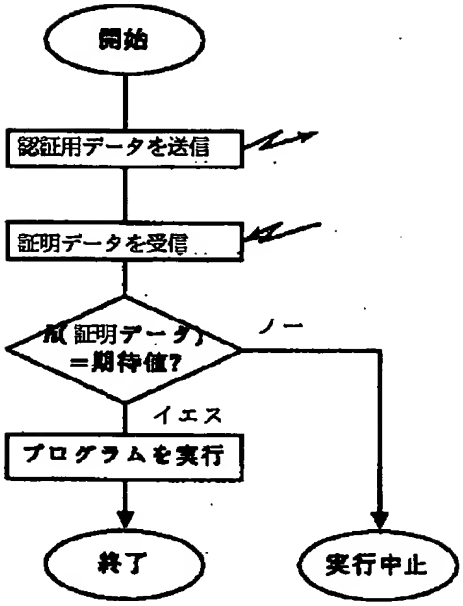
【図6】


認証用素データ記憶
$C' = K^{E} \bmod n$
乱数化
$C = r^{E} \cdot C' \bmod n$
乱数発生
r
アクセスチケット
公開鍵記憶
(E,n)
乱数記憶
r
乱数効果除去
$R = C^{t} \cdot C^{e} \bmod n$
$K' = r^{-1} \cdot R \bmod n$
実行

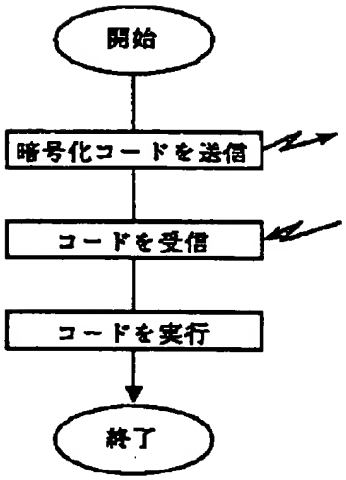
【図8】


開始
認証用データを送信
証明データを受信
証明データ
＝期待値?
ノー
イエス
プログラムを実行
終了
実行中止

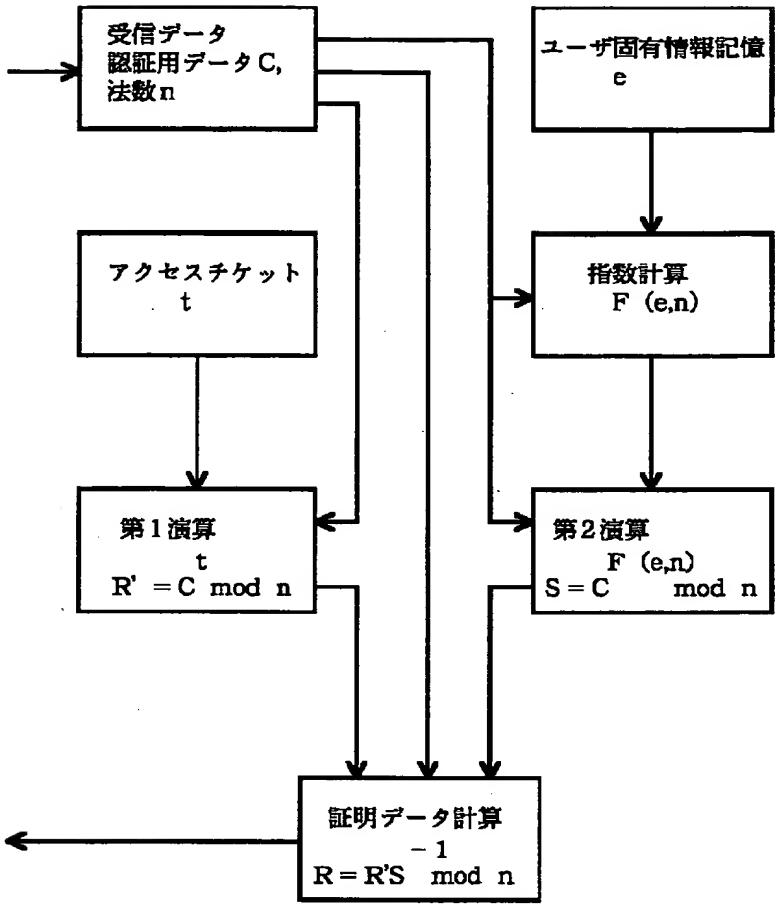
【図10】


開始
認証用データを送信
証明データを受信
証明データ
＝期待値?
ノー
イエス
プログラムを実行
終了
実行中止

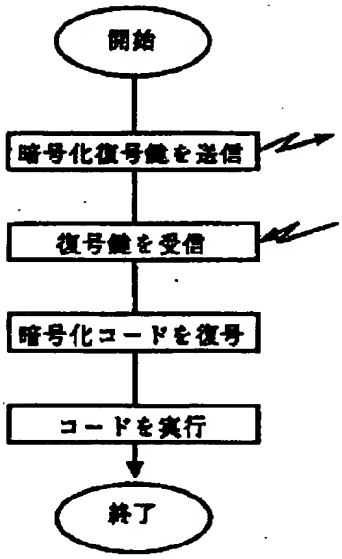
【図12】


開始
暗号化コードを送信
コードを受信
コードを実行
終了

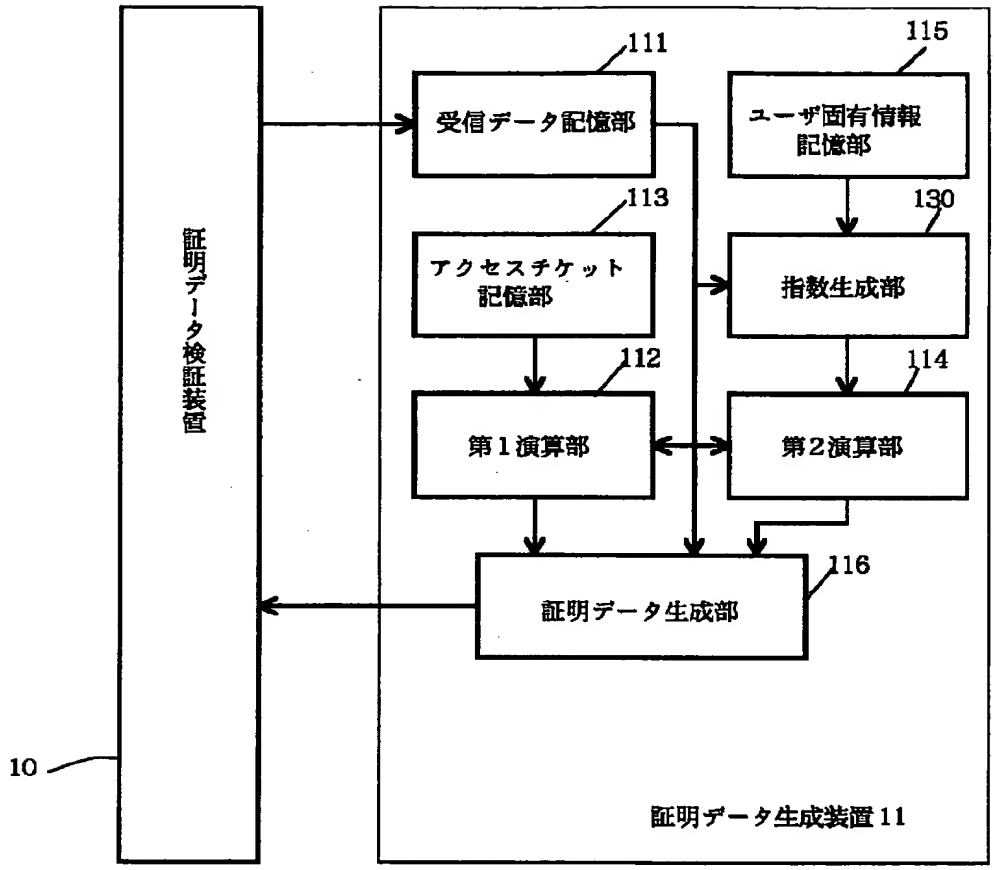
【図16】


受信データ
認証用データC,
法数n
ユーザ固有情報記憶
e
アクセスチケット
t
指数計算
F (e,n)
第1演算
t
R' = C mod n
第2演算
F (e,n)
S = C mod n
証明データ計算
-1
R = R'S mod n

【図14】



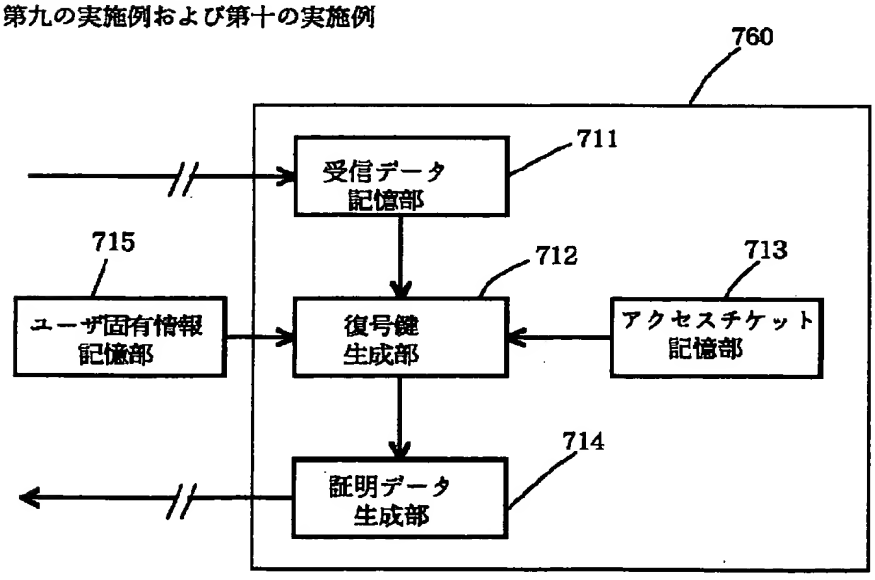
【図15】



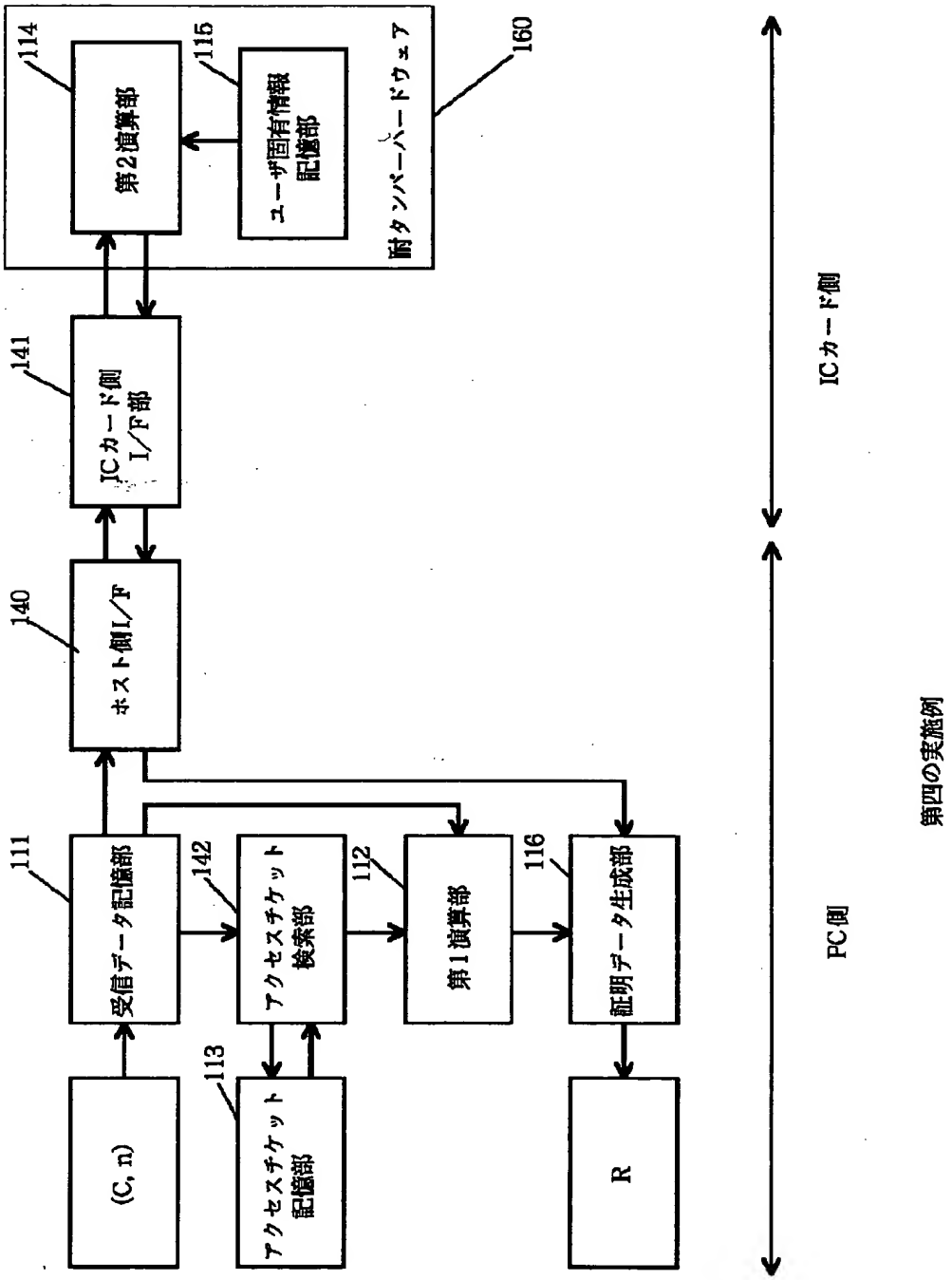
第三の実施例

【図26】

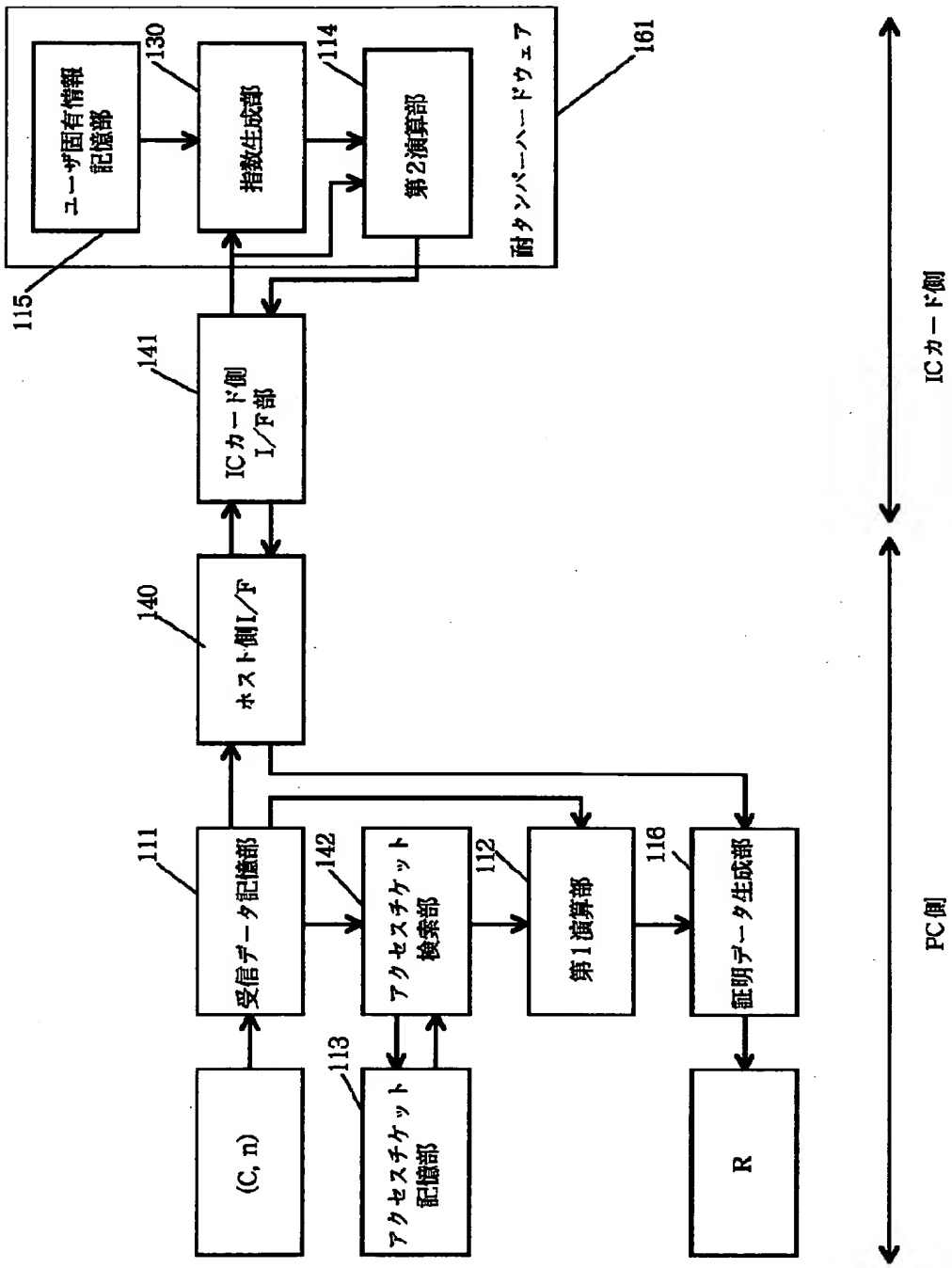
第九の実施例および第十の実施例



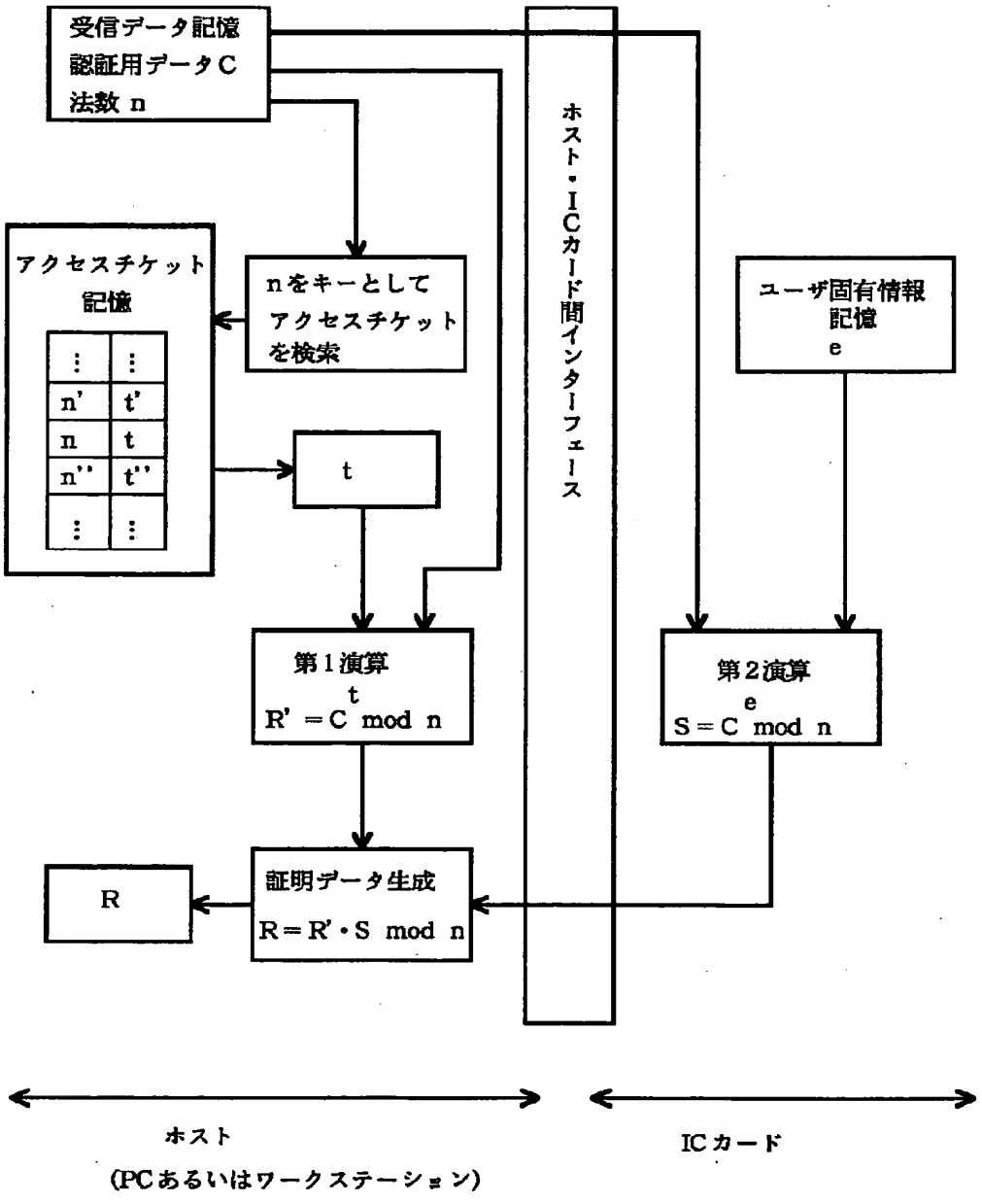
【図17】


114
第2演算部
115
ユーザ固有情報記憶部
160
耐タンパーハードウェア
141
ICカード側I/F部
140
ホスト側I/F
111
受信データ記憶部
142
アクセスチケット検索部
112
第1演算部
116
証明データ生成部
113
アクセスチケット記憶部
(C, n)
R
ICカード側
PC側
第四の実施例

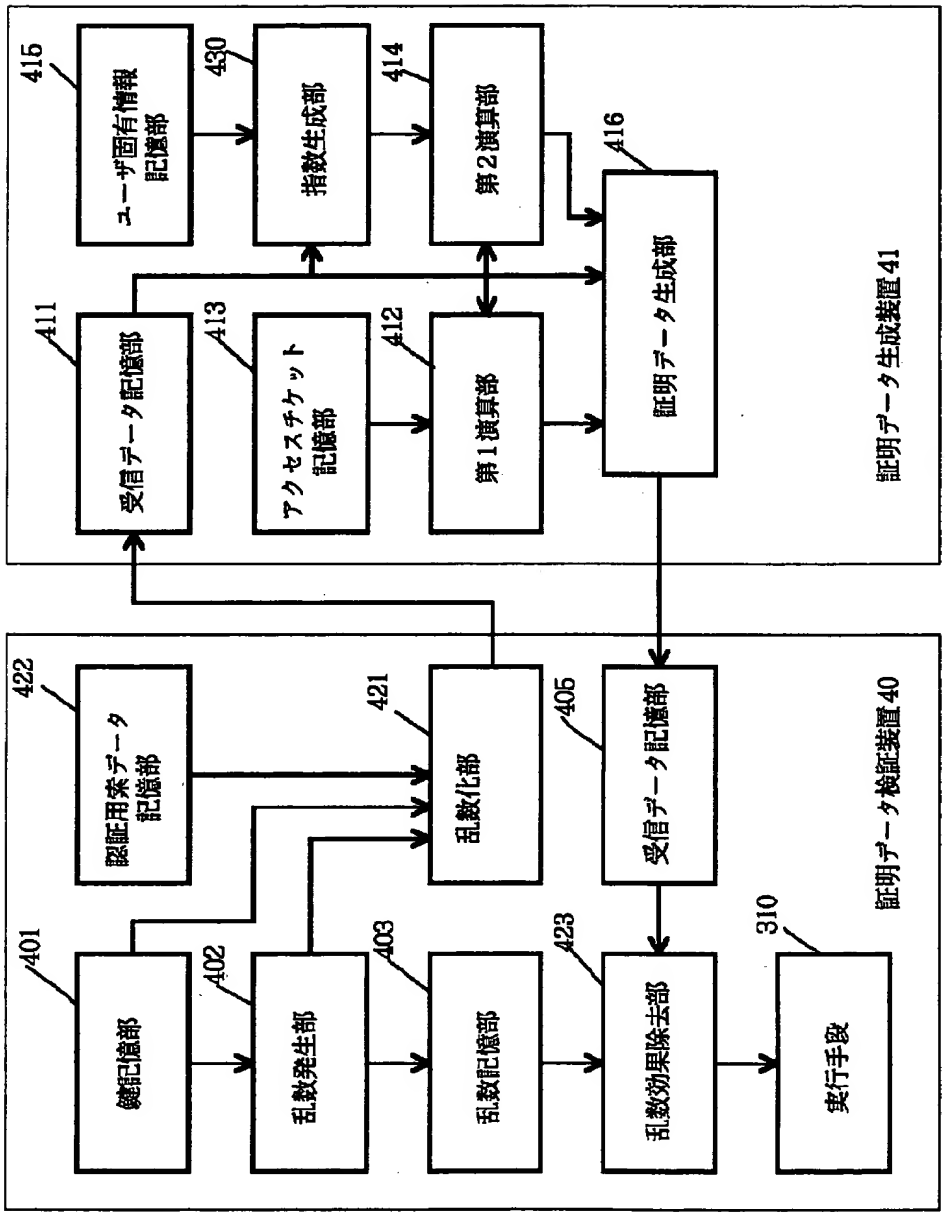
【図18】


耐タンパーハードウェア
161
ユーザ固有情報記憶部
130
指数生成部
114
第2演算部
115
ICカード側I/F部
141
ホスト側I/F
140
受信データ記憶部
111
アクセスチケット検索部
142
第1演算部
112
証明データ生成部
116
(C, n)
アクセスチケット記憶部
113
R
ICカード側
PC側

【図19】

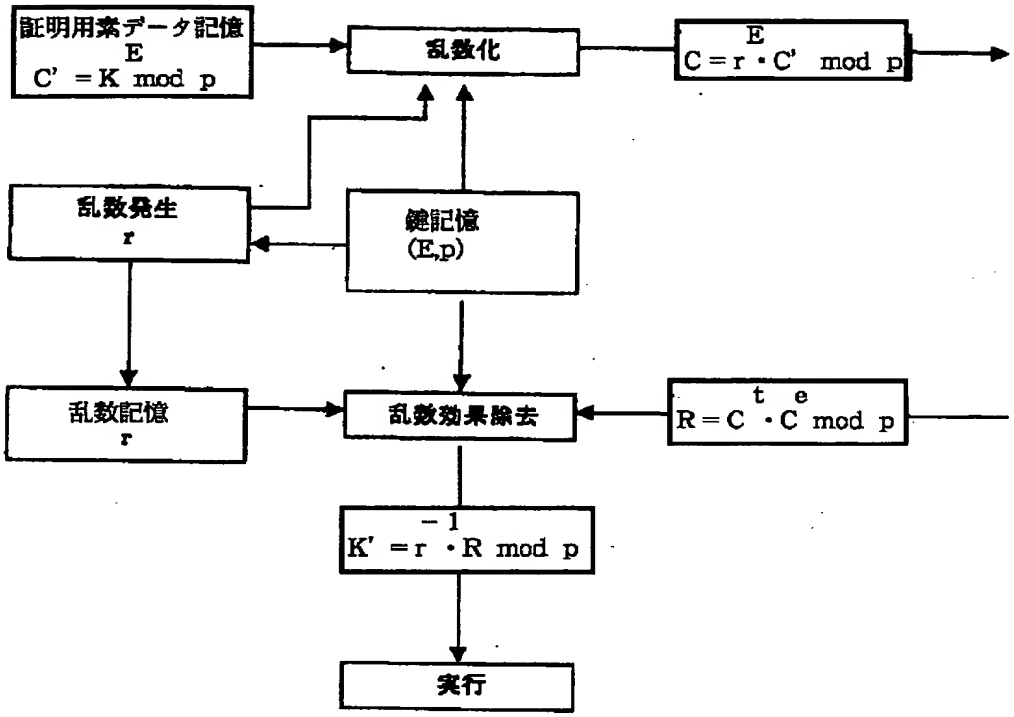

受信データ記憶
認証用データC
法数 n
アクセスチケット
記憶
n'
t'
n
t
n''
t''
nをキーとして
アクセスチケット
を検索
t
第1演算
t
R' ＝C mod n
ホスト・ICカード間インターフェース
ユーザ固有情報
記憶
e
第2演算
e
S＝C mod n
R
証明データ生成
R＝R'・S mod n
ホスト
(PCあるいはワークステーション)
ICカード

【図20】

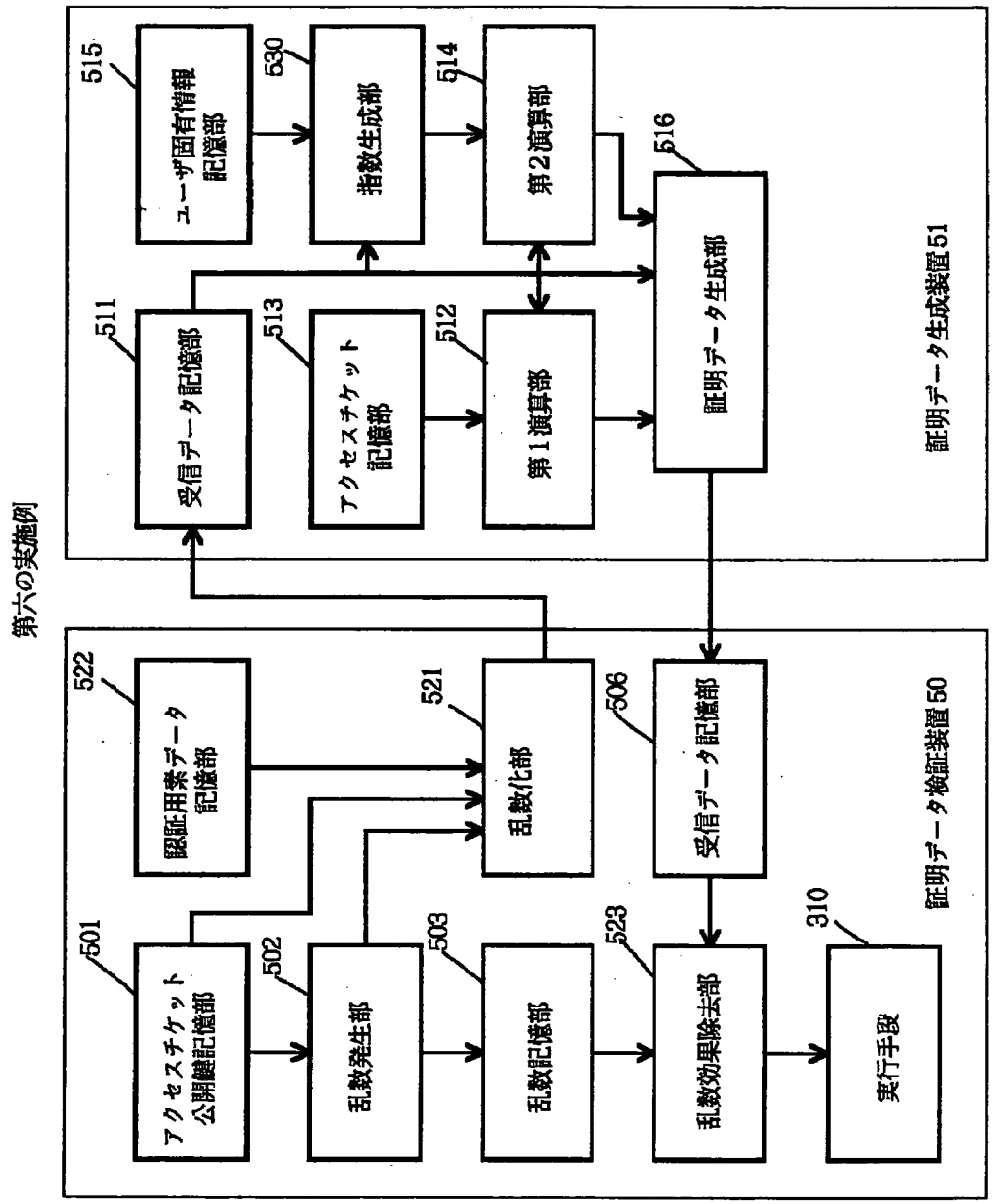

証明データ検証装置40
鍵記憶部
401
乱数発生部
402
乱数記憶部
403
乱数効果除去部
423
実行手段
310
認証用素データ記憶部
422
乱数化部
421
受信データ記憶部
405
証明データ生成装置41
受信データ記憶部
411
アクセスチケット記憶部
413
第1演算部
412
証明データ生成部
416
ユーザ固有情報記憶部
415
指数生成部
430
第2演算部
414

第五の実施例

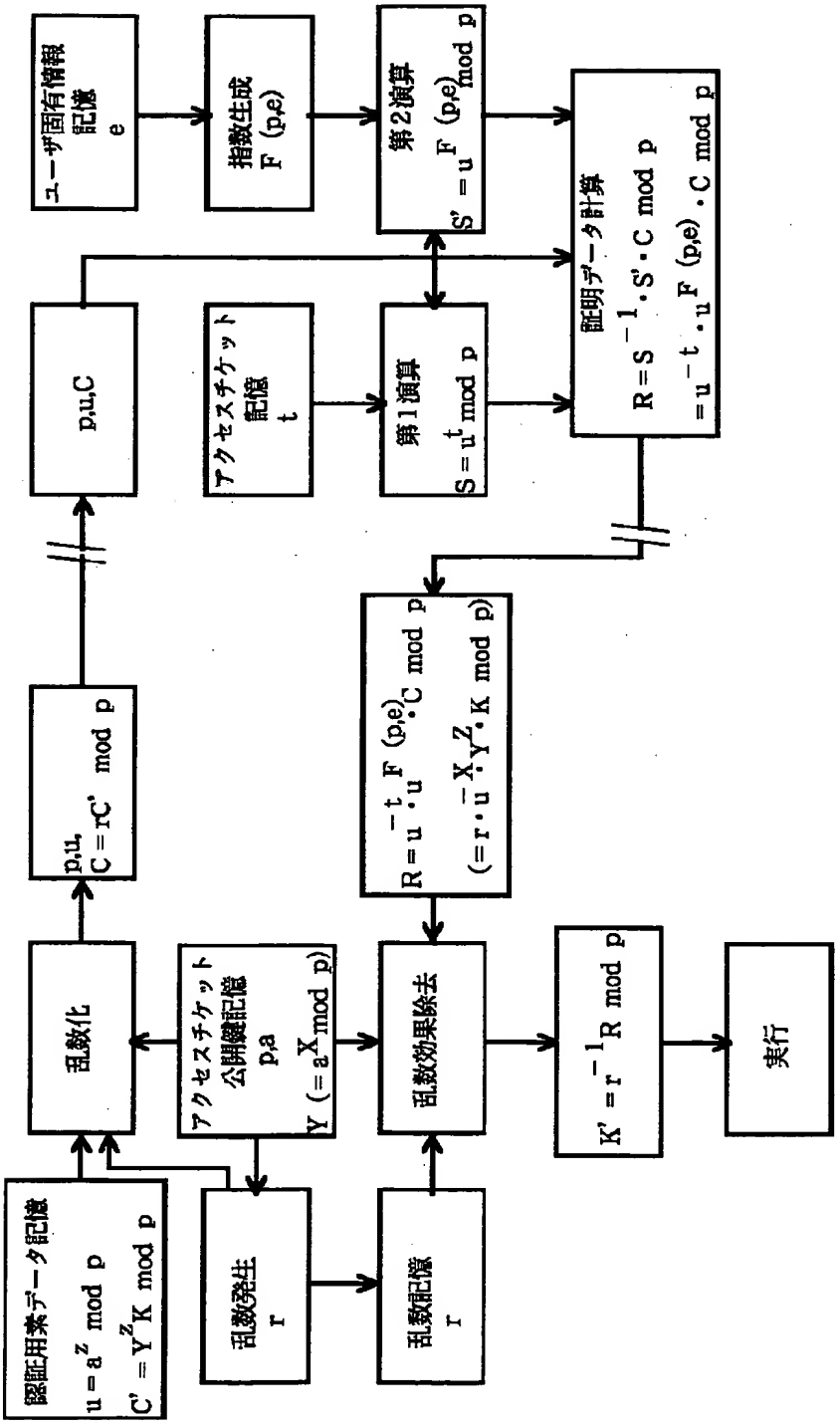
【図21】


証明用素データ記憶
E
C' =K mod p
乱数化
E
C=r・C' mod p
乱数発生
r
鍵記憶
(E,p)
乱数記憶
r
乱数効果除去
t e
R=C ・C mod p
-1
K' =r ・R mod p
実行

【図22】

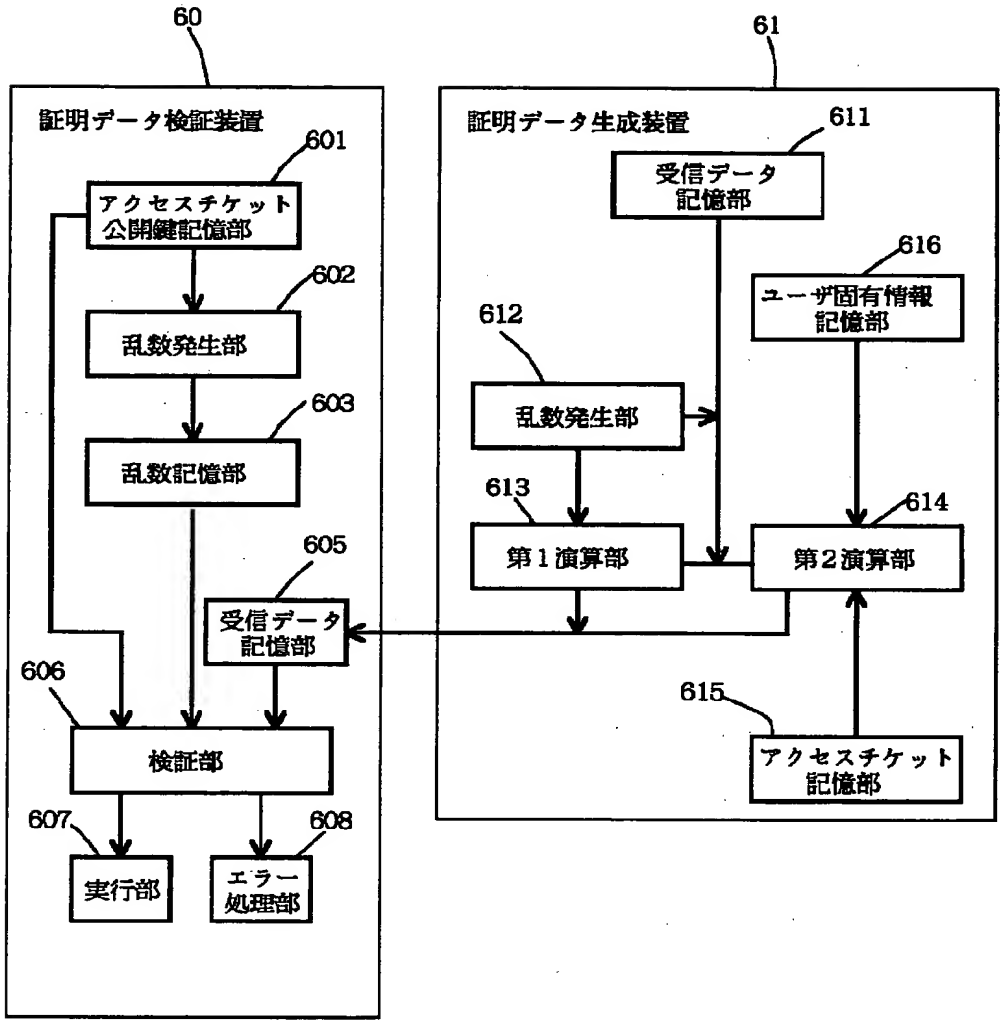

第六の実施例
証明データ生成装置51
ユーザ固有情報記憶部
515
指数生成部
530
第2演算部
514
516
証明データ生成部
受信データ記憶部
511
アクセスチケット記憶部
513
第1演算部
512
証明データ検証装置50
認証用素データ記憶部
522
乱数化部
521
受信データ記憶部
506
アクセスチケット公開鍵記憶部
501
乱数発生部
502
乱数記憶部
503
乱数効果除去部
523
実行手段
310

【図23】

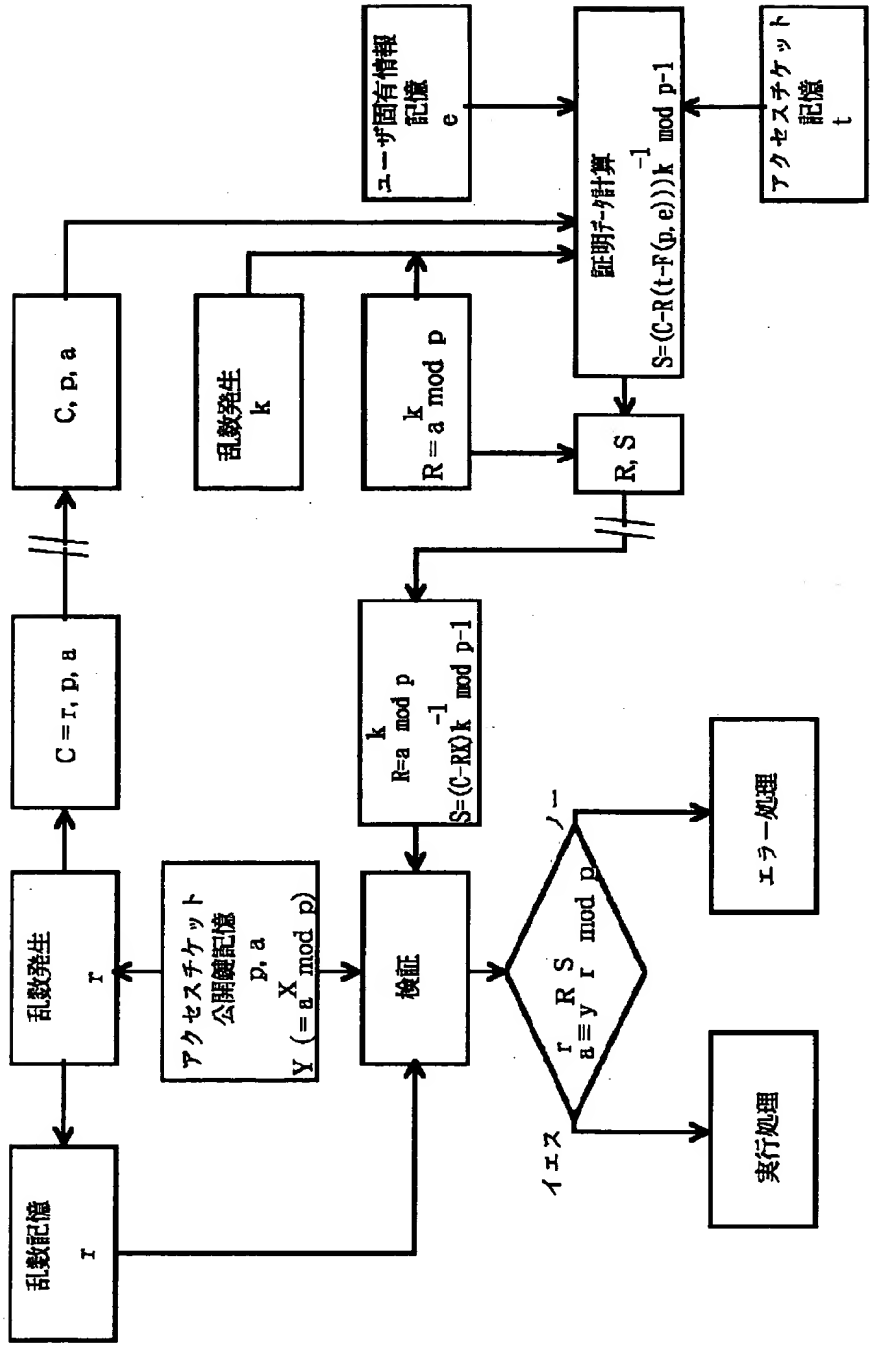

ユーザ固有情報
記憶
e
指数生成
F (p,e)
第2演算
S' = u^F (p,e) mod p
証明データ計算
R = S^-1 · S' · C mod p
= u^-t · u^F (p,e) · C mod p
p,u,C
アクセスチケット
記憶
t
第1演算
S = u^t mod p
p,u,
C = rC' mod p
R = u^-t F (p,e) · C mod p
(= r · u^-X · Y^Z · K mod p)
乱数化
アクセスチケット
公開鍵記憶
p,a
Y (= a^X mod p)
乱数効果除去
K' = r^-1 R mod p
実行
認証用素データ記憶
u = a^Z mod p
C' = Y^Z K mod p
乱数発生
r
乱数記憶
r

【図24】

第七の実施例


60
証明データ検証装置
601
アクセスチケット公開鍵記憶部
602
乱数発生部
603
乱数記憶部
605
受信データ記憶部
606
検証部
607
実行部
608
エラー処理部
61
証明データ生成装置
611
受信データ記憶部
616
ユーザ固有情報記憶部
612
乱数発生部
613
第１演算部
614
第２演算部
615
アクセスチケット記憶部

【図25】



フロントページの続き

(51)Int.Cl.[6]	識別記号	FI	
G06F 12/14	320	G06F 12/14	320A
G09C 1/00	640	G09C 1/00	640B
			640E

H04L 9/00　　675D

English translation of [JP,10-247905,A]
(Publication of Application Nos. 08-62076 and 09-000418)

[Claim(s)]

[Claim 1] In the access rating authentication equipment which attests the above-mentioned user's access rating by verifying the justification of the certification data generated in order to prove a user's access rating The 1st storage means which memorizes the data for authentication, and the 2nd storage means which memorizes a user's proper information, The 3rd storage means which memorizes the auxiliary information for certification which it is as a result of activation that predetermined count was performed, to the above-mentioned user's proper information, and the description information on access rating authentication, The data for authentication currently held at the storage means of the above 1st, and the above-mentioned user's proper information memorized by the storage means of the above 2nd, A certification data generation means to perform predetermined count to the above-mentioned auxiliary information for certification memorized by the storage means of the above 3rd, and to generate certification data, Access rating authentication equipment characterized by having a certification data verification means to verify that the certification data generated by the above-mentioned certification data generation means are generated based on the description information on the above-mentioned access rating authentication.

[Claim 2] Access rating authentication equipment according to claim 1 with which the storage means of the above 2nd and the above-mentioned certification data generation means are characterized by being held in a defense means to close observing internal data and an internal processing procedure from the outside if at least.

[Claim 3] Access rating authentication equipment according to claim 1 characterized by constituting the storage means of the above 2nd, and the above-mentioned certification data generation means as a portable small arithmetic unit of an IC card etc. at least.

[Claim 4] The above-mentioned certification data generation means consists of the 1st operation means and the 2nd operation means. The 1st operation means Predetermined count is performed to a user's proper information memorized by the storage means of the above 2nd, and the auxiliary information for certification memorized by the storage means of the above 3rd. The description information on the above-mentioned access rating authentication is computed as the result. The 2nd operation means Access rating authentication equipment according to claim 1 to 3 characterized by performing predetermined count to the data for authentication memorized by the storage means of

the above 1st, and the description information on the access rating authentication computed by the 1st operation means, and generating the above-mentioned certification data as the result.

[Claim 5] The above-mentioned certification data generation means consists of the 3rd operation means, the 4th operation means, and the 5th operation means. The 3rd operation means Predetermined count is performed to the data for authentication memorized by the storage means of the above 1st, and the auxiliary information for certification memorized by the storage means of the above 3rd. The 4th operation means The count result perform predetermined count to the data for authentication memorized by the storage means of the above 1st, and a user's proper information memorized by the 2nd storage means, and according [the 5th operation means] to the operation means of the above 3rd, Access rating authentication equipment according to claim 1 to 3 characterized by performing predetermined count to the count result by the operation means of the above 4th, and generating the above-mentioned certification data as the result.

[Claim 6] Access rating authentication equipment according to claim 5 with which the storage means of the above 2nd and the operation means of the above 4th are characterized by being held in a defense means to close observing internal data and an internal processing procedure from the outside if at least.

[Claim 7] Access rating authentication equipment according to claim 5 characterized by constituting the storage means of the above 2nd, and the operation means of the above 4th as a portable small arithmetic unit of an IC card etc. at least.

[Claim 8] It is access rating authentication equipment according to claim 1 to 7 the description information on the above-mentioned access rating authentication is a decode key in a code function, and the above-mentioned data for authentication encipher suitable data using the encryption key corresponding to said decode key, and carry out that the above-mentioned certification data-verification means verifies that the above-mentioned certification data which the above-mentioned certification data generation means generates decode the data for authentication correctly as the description.

[Claim 9] Access rating authentication equipment according to claim 1 to 7 characterized by verifying that the above-mentioned certification data which the description information on the above-mentioned access rating authentication is an encryption key in a code function, and the above-mentioned certification data generation means generates encipher the above-mentioned data for authentication correctly using said encryption key.

[Claim 10] Access rating authentication equipment according to claim 1 to 7 characterized by verifying that the above-mentioned certification data which the description information on the above-mentioned access rating authentication is a signature key in a digital signature function, and the above-mentioned certification data generation means generates are the digital signature correctly generated to the above-mentioned data for authentication using said signature key.

[Claim 11] Access rating authentication equipment of a key according to claim 8 or 9 with which an encryption function is an unsymmetrical key code function, and the description information on access rating authentication comes out on the other hand, and it is characterized by a certain thing.

[Claim 12] Access rating authentication equipment according to claim 11 characterized by for an encryption function being a public-key-encryption function, and the description information on access rating authentication being a private key.

[Claim 13] Access rating authentication equipment according to claim 8 or 9 characterized by for an encryption function being a symmetry key code function, and the description information on access rating authentication being a common private key.

[Claim 14] The storage means of the above 1st, the storage means of the above 2nd, and the storage means of the above 3rd, The certification data generation equipment which consists of above-mentioned certification data generation means, and the 4th storage means which memorizes the data for authentication in addition to the above-mentioned certification data verification means, In the access rating authentication equipment with which certification data verification equipment equipped with the 5th storage means which memorizes certification data attests a user's access rating by communicating mutually Certification data verification equipment writes out the data for authentication memorized by the 4th storage means to the 1st storage means of certification data generation equipment. Certification data generation equipment The certification data generated based on the above-mentioned data for authentication written in the 1st storage means by the certification data generation means It is access rating authentication equipment according to claim 1 to 13 which writes out to the 5th storage means in certification data verification equipment, and carries out the description of certification data verification equipment attesting a user's access rating using the above-mentioned certification data written in the 5th storage means.

[Claim 15] The description information on the above-mentioned access rating authentication is the encryption key of an encryption function, and certification data verification equipment is equipped with a random-number generation means. A random-number generation means is written in the 4th storage means by using the

generated random number as the data for authentication. A certification data verification means Access rating authentication equipment according to claim 14 characterized by verifying enciphering the data for authentication whose certification data written in the 5th storage means by certification data generation equipment are said random number with the encryption key which is the description information on access rating authentication.

[Claim 16] The description information on access rating authentication is the decode key of an encryption function. Certification data verification equipment A random-number generation means, While it has the 6th storage means which memorizes the generated random number, and the 7th storage means which memorizes the ** data for authentication and a random-number generation means writes the generated random number in the 6th storage means After giving the random-number effectiveness which used said random number for the ** data for authentication memorized by the 7th storage means, it writes in the 4th storage means as data for authentication. A certification data verification means The result of having removed the random-number effectiveness by the random number memorized by the 6th storage means from the certification data in which it was written by the 5th storage means with the above-mentioned certification data generation equipment Access rating authentication equipment according to claim 14 characterized by verifying decoding the ** data for authentication memorized by the 7th storage means with the decode key which is the description information on access rating authentication.

[Claim 17] The description information on the above-mentioned access rating authentication is the signature key of a digital signature function. Certification data verification equipment is equipped with a random-number generation means, and a random-number generation means is written in the 4th storage means by using the generated random number as the data for authentication. A certification data verification means Access rating authentication equipment according to claim 14 characterized by verifying that the certification data written in the 5th storage means by certification data generation equipment are a digital signature with the signature key it is [key] the description information on access rating authentication to the data for authentication which are said random number.

[Claim 18] An encryption function is the RSA public key encryption under Law n, the description information on access rating authentication is a private key D, and the public key corresponding to a private key D is E. A certification data verification means The certification data R written in the 5th storage means E the data C for authentication remembered to be the squared result by the 4th storage means Access

rating authentication equipment according to claim 15 characterized by verifying a congruent thing (RE mod n = C mod n) by the basis which is Law n.

[Claim 19] An encryption function is the RSA public key encryption under Law n, and the description information on access rating authentication is a private key D. It is squared several K' (=KE mod n) E under n. the ** data for authentication which the public key corresponding to a private key D is E, and are memorized by the storage means of the above 7th -- Data K -- law -- the random number r which generated the above-mentioned random-number generation means -- law -- with the number squared E under n It writes in said 4th storage means by using as the data for authentication several C (=rEK' mod n) by which it multiplied under n. said K' -- law -- a certification data verification means the law of the random number r memorized by the 6th storage means -- with the number which multiplied the certification data R in which it was written by the 5th storage means with certification data generation equipment by the inverse number under n Access rating authentication equipment according to claim 16 characterized by verifying that said K is congruent under Law n (K mod n=r-1R mod n).

[Claim 20] An encryption function is the RSA public key encryption under Law n, and the description information on access rating authentication is a private key D. The auxiliary information t for certification which the public key corresponding to a private key D is E, and is memorized by the storage means of the above 3rd A user's proper information e memorized by the storage means of the above 2nd is subtracted from said D. It is data (t=D-e+omegaphi (n)) which add a product with Euler number [of the un-colliding nature function values omega (=G (n, e)) and n] phi (n) depending on said n and e, and are obtained. The above-mentioned certification data generation means Furthermore, said t, the law from the data C for authentication written in said e and the 1st storage means -- the access rating authentication equipment according to claim 18 or 19 characterized by generating said certification data by calculating the Dth power (CD mod n) of C under n.

[Claim 21] The above-mentioned certification data generation means consists of the 3rd operation means, the 4th operation means, and the 5th operation means. The 3rd operation means Said t-th power (Ct mod n) of said C is calculated under the describing [above] method n. The 4th operation means Said e-th power (Ce mod n) of said C is calculated under the describing [above] method n. The 5th operation means Access rating authentication equipment according to claim 20 characterized by generating the certification data R (=CtCe mod n) by multiplying by the count result of the 1st and 2nd operation means under the describing [above] method n.

[Claim 22] Access rating authentication equipment according to claim 21 characterized

by building in said 2nd storage means and said 4th operation means in a defense means to defend an internal processing procedure and data from external observation.

[Claim 23] An encryption function is the RSA public key encryption under Law n, and the description information on access rating authentication is a private key D. The auxiliary information t for certification which the public key corresponding to a private key D is E, and is memorized by the storage means of the above 3rd It is data (t=D+F (n, e)) which add the un-colliding nature function value F depending on proper information e and said law n of the user memorized by the storage means of the above 2nd (n, e) to said D, and are obtained. The above-mentioned certification data generation means Said t, the law from the data C for authentication written in said e and said 1st storage means -- the access rating authentication equipment according to claim 18 or 19 characterized by generating said certification data by calculating the Dth power (CD mod n) of C under n.

[Claim 24] The above-mentioned certification data generation means consists of the 3rd operation means, the 4th operation means, and the 5th operation means. The 3rd operation means Said t-th power (Ct mod n) of said C is calculated under the describing [above] method n. The 4th operation means Said F (n, e) ** (CF(n, e) mod n) of said C is calculated under the describing [above] method n. The 5th operation means Access rating authentication equipment according to claim 23 characterized by generating the certification data R (=CtC-F(n, e) mod n) under the describing [above] method n by multiplying by the inverse number of the count result of the 3rd operation means, and the count result of the 4th operation means.

[Claim 25] Access rating authentication equipment according to claim 24 characterized by building in said 2nd storage means and said 4th operation means in a defense means to defend an internal processing procedure and data from external observation.

[Claim 26] An encryption function is a Pohlig-Hellman unsymmetrical key code under Law p. The description information on access rating authentication is one key D, and the key of another side corresponding to Key D is E (DE mod p-1 = 1). A certification data verification means The certification data R written in the 5th storage means E The squared result, the data C for authentication memorized by the 4th storage means -- law -- the access rating authentication equipment according to claim 15 characterized by verifying a congruent thing (RE mod p = C mod p) under p.

[Claim 27] An encryption function is a Pohlig-Hellman unsymmetrical key code under Law p. The description information on access rating authentication is one key D, and the key of another side corresponding to Key D is E (DE mod p-1 = 1). It is squared several K' (=KE mod p) E under p. the ** data for authentication memorized by the

storage means of the above 7th -- Data K -- law -- the above-mentioned random-number generation means It writes in said 4th storage means by using as the data for authentication several C (=rEK' mod p) by which it multiplied under p. the generated random number r -- law -- the number squared E under p, and said K' -- law -- the law of the random number r with which the certification data verification means is memorized by the 6th storage means -- with the number which multiplied the certification data R in which it was written by the 5th storage means with certification data generation equipment by the inverse number under p Access rating authentication equipment according to claim 16 characterized by verifying that said K is congruent under Law p (K mod p=r-1R mod p).

[Claim 28] An encryption function is a Pohlig-Hellman unsymmetrical key code under Law p. The description information on access rating authentication is one key D, and the key of another side corresponding to Key D is E (DE mod p-1 = 1). It is data (t=D+F (p, e)) with which the auxiliary information t for certification memorized by the storage means of the above 3rd adds the un-colliding nature function value F depending on the user proper information e memorized by the storage means of the above 2nd, and said p (p, e) to said D, and is acquired. The above-mentioned certification data generation means Said t, the law from the data C for authentication written in said e and the 1st storage means -- the access rating authentication equipment according to claim 26 or 27 characterized by generating said certification data by calculating the Dth power (CD mod p) of C under p.

[Claim 29] The above-mentioned certification data generation means consists of the 3rd operation means, the 4th operation means, and the 5th operation means. The 3rd operation means Said t-th power (Ct mod p) of said C is calculated under the describing [above] method p. The 4th operation means Under the describing [above] method p, the exponentiation (CF(p, e) mod p) of said C is calculated by making said F (p, e) into a characteristic. The 5th operation means Access rating authentication equipment according to claim 28 characterized by generating the certification data R (=CtC-F(p, e) mod p) under the describing [above] method p by multiplying by the inverse number of the count result of the 3rd operation means, and the count result of the 4th operation means.

[Claim 30] Access rating authentication equipment according to claim 29 characterized by building in said 2nd storage means and said 4th operation means in a defense means to defend an internal computational procedure and data from external observation.

[Claim 31] Encryption functions are Law p and the ElGamal public key encryption under Generator a. The description information on access rating authentication is one

key X, and the public key corresponding to Key X is Y (Y = aX mod p). u -- Above a -- law -- the number which made the suitable random number z the characteristic and carried out the exponentiation under p -- it is (u=az mod p) -- K' -- Above Y -- law -- with the number which made the above-mentioned random number z the characteristic, and carried out the exponentiation under p When it is a product with Data K (K'=YzK mod p), the group of u and K' is memorized by the storage means of the above 7th as ** data for authentication. The above-mentioned random-number generation means It writes in said 4th storage means by using as the data for authentication several C (=rK' modp) by which it multiplied under p. Above u and the generated random number r -- said K' -- law -- a certification data verification means the law of the random number r memorized by the 6th storage means -- with the number which multiplied the certification data R in which it was written by the 5th storage means with certification data generation equipment by the inverse number under p Access rating authentication equipment according to claim 16 characterized by verifying that said K is congruent under Law p (K mod p=r-1R mod p).

[Claim 32] Encryption functions are Law p and the ElGamal public key encryption under Generator a. The description information on access rating authentication is one key X, and the public key corresponding to Key X is Y (Y = aX mod p). It is data (t=X+F (p, e)) with which the auxiliary information t for certification memorized by the storage means of the above 3rd adds the un-colliding nature function value F depending on the user proper information e memorized by the storage means of the above 2nd, and said p (p, e) to said X, and is acquired. The above-mentioned certification data generation means Said t, the law from the data u and C for authentication written in said e and the 1st storage means -- the access rating authentication equipment according to claim 31 characterized by generating the above-mentioned certification data by calculating under p the number (Cu-X mod p) which broke C by the Xth power of Above u.

[Claim 33] The above-mentioned certification data generation means consists of the 3rd operation means, the 4th operation means, and the 5th operation means. The 3rd operation means Said t-th power (ut mod p) of said u is calculated under the describing [above] method p. The 4th operation means Said F (p, e) ** (uF(p, e) mod n) of said u is calculated under the describing [above] method p. The 5th operation means Access rating authentication equipment according to claim 32 characterized by generating the certification data R (=Cu-tuF(p, e) mod p) by being as a result of [of the 3rd operation means] count, breaking Above C under the describing [above] method p, and multiplying by the count result of the 4th operation means further.

[Claim 34] Access rating authentication equipment according to claim 33 characterized

by building in said 2nd storage means and said 4th operation means in a defense means to defend an internal computational procedure and data from external observation.

[Claim 35] A signature function is the ElGamal signature under Law p and Generator a, and the description information on access rating authentication is one key X. The public key corresponding to Key X is Y (Y = aX mod p). A certification data verification means the certification data R and S written in the 5th storage means -- receiving -- law -- under p The value which made the characteristic the data C for authentication memorized by the 4th storage means in Above a, and carried out the exponentiation, the product of the value which squared Above Y R, and the value which squared R S -- law -- the access rating authentication equipment according to claim 17 characterized by verifying a congruent thing (aC mod p = YRRS mod p) under p.

[Claim 36] A signature function is the ElGamal signature under Law p and Generator a, and the description information on access rating authentication is one key X. The public key corresponding to Key X is Y (Y = aX mod p). It is data (t=X+F (p, e)) with which the auxiliary information t for certification memorized by the storage means of the above 3rd adds the un-colliding nature function value F depending on the user proper information e memorized by the storage means of the above 2nd, and said p (p, e) to said X, and is acquired. The above-mentioned certification data generation means The k-th power of the above a under p is set to R (=ak mod p). the certification data R and S -- generating -- hitting -- the suitable random number k -- generating -- law -- with said t Under law p-1 from the data C for authentication written in said e and the 1st storage means Access rating authentication equipment according to claim 35 characterized by calculating S (=(C-RX) k-1 mod p-1) by multiplying the number which lengthened the product of X and r from C by the inverse number of k.

[Claim 37] Access rating authentication equipment according to claim 36 characterized by building in the 2nd storage means and a certification data generation means in a defense means to defend an internal computational procedure and data from external observation.

[Claim 38] When the above-mentioned user's proper information is the decode key of a code function, the auxiliary information for certification enciphers the description information for access rating authentication with the encryption key corresponding to said decode key and the 1st operation means decodes the auxiliary information for certification using the decode key which is the above-mentioned user's proper information, it is access rating authentication equipment according to claim 4 which carries out [computing the description information for access rating authentication, and] as the description.

[Claim 39] Access rating authentication equipment according to claim 38 characterized by for the above-mentioned code function being an unsymmetrical key code function, and a user's proper information being one key.

[Claim 40] Access rating authentication equipment according to claim 39 characterized by for the above-mentioned code function being a public-key-encryption function, and a user's proper information being a private key.

[Claim 41] Access rating authentication equipment according to claim 38 characterized by for the above-mentioned code function being a symmetry key code function, and a user's proper information being a common private key.

[Claim 42] The 8th storage means which memorizes the plaintext data corresponding to the above-mentioned data for authentication or the above-mentioned ** data for authentication with which the above-mentioned certification data verification means was enciphered, and which is data, The result of having removed the random-number effectiveness from the above-mentioned certification data with which it has a comparison means and the above-mentioned certification data generation means generated the above-mentioned comparison means, or certification data, Access rating authentication equipment according to claim 8 or 16 characterized by comparing the plaintext data memorized by the 8th storage means, restricting when both are in agreement, and judging that the above-mentioned certification data are just.

[Claim 43] The 9th storage means which memorizes the result of having given the predetermined one-way function to the plaintext data corresponding to the above-mentioned data for authentication or the above-mentioned ** data for authentication with which the above-mentioned certification data verification means was enciphered, and which is data, It has the 6th operation means and comparison means which performs a top Norikazu directional function. The 6th operation means If required for the above-mentioned certification data which the above-mentioned certification data generation means generated, after removing the random-number effectiveness, a one-way function is given. The above-mentioned comparison means Access rating authentication equipment according to claim 8 or 16 characterized by comparing the data remembered to be a count result by the 6th operation means by the 9th storage means, restricting when both are in agreement, and judging that the above-mentioned certification data are just.

[Claim 44] The above-mentioned certification data verification means includes a program execution means. The above-mentioned data for authentication, or the above-mentioned ** data for authentication It is data which encipher a program and are obtained. The above-mentioned certification data verification means If required in the

above-mentioned certification data which the certification data generation means generated, after removing the random-number effectiveness, by handing over for a program execution means as a program When a certification data generation means decodes correctly the enciphered above-mentioned data for authentication or the ** data for authentication which is a program, Namely, access rating authentication equipment according to claim 8 or 16 characterized by restricting when the enciphered program is decoded correctly, and a program execution means performing right actuation.

[Claim 45] The program the above-mentioned certification data verification means is remembered to be by the program store means including the program execution means, the program store means, and the program decode means The part or all is enciphered. The above-mentioned data for authentication, or the above-mentioned ** data for authentication It is data which encipher separately the decode key for decoding said enciphered program, and are obtained. The above-mentioned certification data verification means The above-mentioned certification data which the certification data generation means generated are handed over for a program decode means. A program decode means If required in the certification data which said certification data generation means generated, after removing the random-number effectiveness, by using as a decode key By performing the program which decodes the required part of the program memorized by the program store means and by which the program execution means was decoded When a certification data generation means decodes correctly the above-mentioned data for authentication, or the ** data for authentication, Namely, access rating authentication equipment according to claim 8 or 16 characterized by restricting when a decode key is decoded correctly, in order to decode the enciphered program, and a program execution means performing right actuation.

[Claim 46] Access rating authentication equipment according to claim 14 which communicates without forming the above-mentioned certification data generation equipment and the above-mentioned certification data authentication equipment in the same housing, and the above-mentioned certification data generation equipment and the above-mentioned certification data authentication equipment understanding the communication media of the exterior of the housing concerned.

[Claim 47] In the access rating authentication approach which attests the above-mentioned user's access rating by verifying the justification of the certification data generated from the data for authentication in order to prove a user's access rating The step which memorizes the above-mentioned data for authentication, and the step which memorizes a user's proper information, The step which memorizes the auxiliary information for certification which it is as a result of activation that predetermined

count was performed, to the above-mentioned user's proper information, and the description information on access rating authentication, The step which performs predetermined count to the above-mentioned data for authentication, the above-mentioned user's proper information, and the above-mentioned auxiliary information for certification, and generates certification data, The access rating authentication approach characterized by having the step which verifies that the certification data generated by the above-mentioned certification data generation means are generated based on the description information on the above-mentioned access rating authentication.

[Claim 48] In order to attest the above-mentioned user's access rating by verifying the justification of the certification data generated from the data for authentication in order to prove a user's access rating In the program product for access rating authentication used by computer The step which memorizes the above-mentioned data for authentication, and the step which memorizes a user's proper information, The step which memorizes the auxiliary information for certification which it is as a result of activation that predetermined count was performed, to the above-mentioned user's proper information, and the description information on access rating authentication, The step which performs predetermined count to the above-mentioned data for authentication, the above-mentioned user's proper information, and the above-mentioned auxiliary information for certification, and generates certification data, The program product for access rating authentication characterized by using the step which verifies that the certification data generated by the above-mentioned certification data generation means are generated based on the description information on the above-mentioned access rating authentication for performing the above-mentioned computer.

[Claim 49] In order to generate from the data for authentication, the certification data which have the justification verified in order to attest a user's access rating In the program product for certification data generation used by computer The step which memorizes the above-mentioned data for authentication, and the step which memorizes a user's proper information, The step which memorizes the auxiliary information for certification which it is as a result of activation that predetermined count was performed, to the above-mentioned user's proper information, and the description information on access rating authentication, The program product for certification data generation characterized by being used for making the above-mentioned computer perform the step which performs predetermined count to the above-mentioned data for authentication, the above-mentioned user's proper information, and the

above-mentioned auxiliary information for certification, and generates certification data.

[Claim 50] In the program execution control unit which attests the above-mentioned user's access rating and controls program execution based on authentication of the above-mentioned rating by verifying the justification of the certification data generated in order to prove a user's access rating The 1st storage means which memorizes the data for authentication, and the 2nd storage means which memorizes a user's proper information, The 3rd storage means which memorizes the auxiliary information for certification which it is as a result of activation that predetermined count was performed, to the above-mentioned user's proper information, and the description information on access rating authentication, The above-mentioned user's proper information memorized by the storage means of the above 2nd and the above-mentioned auxiliary information for certification memorized by the storage means of the above 3rd are used. A certification data generation means to generate the above-mentioned certification data from the above-mentioned data for authentication, The program execution control unit characterized by having a means to verify the justification of the certification data generated from the above-mentioned certification data generation means, and a means to continue program execution when the justification of the above-mentioned certification data is verified.

[Claim 51] In the information processor which attests the above-mentioned user's access rating and permits access to the above-mentioned predetermined information processing resource by verifying the justification of the certification data generated in order to prove access rating of the user to a predetermined information processing resource The 1st storage means which memorizes the data for authentication, and the 2nd storage means which memorizes a user's proper information, The 3rd storage means which memorizes the auxiliary information for certification which it is as a result of activation that predetermined count was performed, to the above-mentioned user's proper information, and the description information on access rating authentication, The above-mentioned user's proper information memorized by the storage means of the above 2nd and the above-mentioned auxiliary information for certification memorized by the storage means of the above 3rd are used. A certification data generation means to generate the above-mentioned certification data from the above-mentioned data for authentication, The information processor characterized by having a means to verify the justification of the certification data generated from the above-mentioned certification data generation means, and a means to permit access to the above-mentioned predetermined information processing resource based on

verification of the above-mentioned justification.

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the access rating authentication equipment and the approach of attesting a user's access rating.

[0002]

[Description of the Prior Art]

[Related technique] The program execution control technique is known as advanced technology belonging to this invention and an isomerism field. The user who has tried activation of application inspects holding the key for authentication of normal, a program execution control technique embeds the routine for a user's access rating authentication into 1. application program, 2. this routine restricts it, when existence of the key for the 3. above-mentioned authentication is checked, it continues a program, and when other, it is the technique which stops program execution. By using this technique, activation of an application program can be closed to him, if only to the user of the normal which holds an authentication key. It is put in practical use in the software distribution enterprise and this technique is Rainbow as a product. Technologies, Sentinel of an Inc. company SuperPro (trademark) and Aladdin Knowledge There is an HASP (trademark) of a SystemssLtd. company etc.

[0003] A program execution control technique is explained more below at a detail.

1. The user who performs software holds an authentication key as user proper information. An authentication key is a key for encryption and those who permit use of software, for example, a software vendor, distribute it to a user. An authentication key is severely enclosed with the memory in hardware etc., in order to prevent a duplicate, and it is delivered by the user using a postal physical means.

2. A user equips a proprietary personal computer workstation by the approach which had the hardware which built in the authentication key specified. A printer port is equipped with hardware.

3. If a user starts an application program and program execution attains to the above-mentioned access rating authentication routine, a program will communicate with the hardware which built in a user's authentication key. If a program identifies an authentication key and existence of a right authentication key is checked based on the result of a communication link, activation will be moved to the following step. When a communication link goes wrong and existence of an authentication key cannot be checked, a program stops oneself and can be made not to perform subsequent activation.

[0004] Discernment of the authentication key by the access rating authentication routine is performed according to the following protocols, for example.

1. An access rating authentication routine generates a suitable number, and transmits to hardware with a built-in key.

2. The hardware with a built-in key enciphers the number sent using the authentication key to build in, and answers the above-mentioned access rating authentication routine.

3. An authentication routine judges whether it is the number with which the answered number enciphers the number expected beforehand, i.e., the number transmitted to hardware, with a right authentication key, and is obtained.

4. In being in agreement with the number with which the answered number was expected, it continues program execution, and in not being in agreement, it stops.

[0005] Under the present circumstances, even if the communication link between an application program and hardware with a built-in authentication key is exchanged between the same hardware in the same part in the same application program, they must differ at every activation. Otherwise, it will also enable the user who does not hold a right authentication key to perform a program by performing the reply to an application program as it recorded the contents of a communication link in a normal activation process once, and it recorded, whenever it performed the program after that. Unjust activation of the application program by reappearance of such contents of a communication link is called a replay attack (replay attack).

[0006] In order to prevent a replay attack, the number sent to hardware with a built-in key usually uses the random number newly generated at every communication link.

[0007] The trouble of the [trouble of conventional technique] conventional technique originates in the property in which protection processing of a program must be performed based on this authentication key, after a programmer assumes beforehand the authentication key which a user has, when creating an application program. That is, only when the right reply from hardware with a built-in key is predicted at the time of a programming and a right reply is received, a programmer has to create a program so that a program may be performed normally.

[0008] Although the use gestalt of the conventional technique of having the above-mentioned description becomes two kinds fundamentally, it has the problem which states below in any case.

[0009] 1. In a primary method, prepare a user's authentication key so that it may differ for every user. That is, every one different authentication key for every user is prepared for the user first like authentication **** at authentication **** and the user second.

[0010] In this case, a programmer needs to change the authentication routine in a

program appropriately for every user, and needs to create a program. That is, since authentication keys differ for every user, the authentication routine in a program must be created so that the authentication key of the user proper using this program may be identified, and a programmer needs to create the program from which only the number of use users differs.

[0011] When the target users are a large number, the activity which changes a program an individual exception for every user requires an effort intolerable for a programmer, and becomes what also has a huge list of user authentication keys which must be managed.

[0012] 2. By the second approach, a programmer prepares an authentication key which is different for every application, respectively. That is, every one authentication key which is different for every application like authentication **** is prepared for the application first at authentication **** and the application second, and each application program is created so that the authentication key of a proper may be identified.

[0013] Although the need of creating a program individually for every user like [in the case of a primary method] is lost by this approach, as for a user, only the number of the applications to be used must hold an authentication key conversely.

[0014] As for this constraint, the following problems are caused in a programmer and each user.

[0015] As mentioned above, it is necessary to distribute an authentication key to a user in the condition of having enclosed with hardware severely. Therefore, it cannot but depend for distribution of the hardware which builds in an authentication key on physical means, such as mail, to the ability to distribute the program itself simple through a network. the hardware with which the authentication key corresponding to this application whenever a programmer receives since [use consent / of application] from a user was enclosed -- it is necessary to mail -- cost, time amount, and the time and effort of packing -- any -- very much -- a programmer -- **** -- it becomes a big burden.

[0016] A programmer has to do the fixed number stock of the different hardware for every application so that he may meet the demand of a user, and he needs the cost of stock control.

[0017] Moreover, a user must be content with the complicatedness that hardware must be exchanged whenever it changes the application to be used.

[0018] Though he wants to use application with a user, it must wait until the hardware with which the authentication key was enclosed is mailed, and there is also inconvenience that it cannot use immediately.

[0019] The method of teaching a user the password for making the intact authentication

key in hardware available, whenever it encloses two or more authentication keys beforehand into hardware and permits a user use of new application, in order to mitigate this burden is used. However, even if it uses this approach, the above-mentioned trouble's not being solved theoretically is clear. On the occasion of commercialization, hardware is designed so that more than one may be enabled to connect and to join together, and it has actually eased inconvenient [resulting from the above-mentioned trouble].

[0020] Thus, even if it takes which [above-mentioned / two] approach, a problem exists in the convenience of a programmer and a user.

[0021] In addition, considering the external special feature of execution control, it can imagine [that it is applicable also to the access control of privacy protection and the file of e-mail, or a computer resource, and]. However, even if it is going to apply the conventional technique to these fields, it is impossible by the above-mentioned trouble.

[0022]

[Problem(s) to be Solved by the Invention] In case it cancels and has the both sides by the side of a user and an application implementer's etc. protection and program execution control, the privacy protection of e-mail, a file, the access control of a computer resource, etc. are performed from the fault derived from this invention being made in consideration of the above situation, and dealing with proper information, such as many authentication keys, it aims at offering the access rating authentication technique which enabled it to attest a user's access rating simply.

[0023]

[Means for Solving the Problem] To the access rating authentication equipment which attests the above-mentioned user's access rating by verifying the justification of the certification data generated in order to prove a user's access rating in order to attain the above-mentioned purpose according to the 1st side face of this invention The 1st storage means which memorizes the data for authentication, and the 2nd storage means which memorizes a user's proper information, The 3rd storage means which memorizes the auxiliary information for certification which it is as a result of activation that predetermined count was performed, to the above-mentioned user's proper information, and the description information on access rating authentication, The data for authentication currently held at the storage means of the above 1st, and the above-mentioned user's proper information memorized by the storage means of the above 2nd, A certification data generation means to perform predetermined count to the above-mentioned auxiliary information for certification memorized by the storage means of the above 3rd, and to generate certification data, He is trying to establish a

certification data verification means to verify that the certification data generated by the above-mentioned certification data generation means are generated based on the description information on the above-mentioned access rating authentication.

[0024] According to this configuration, the description information for access rating authentication which is a protection side and is given, and the user proper information given to a user side can be made to become independent by introducing the auxiliary data for certification (access ticket). Access rating of users, such as execution control, can be attested by a user's possessing user proper information beforehand, and protection persons', such as a programmer's, preparing the description information on access rating authentication independently of the user proper information which a user possesses, and creating an access ticket according to a user's proper information and the description information on access rating authentication used for creation of an application program etc., and distributing. Thus, the complicatedness produced when a user and a protection side attest using the same information is avoidable.

[0025] Moreover, in this configuration, the storage means of the above 2nd and the above-mentioned certification data generation means may be made to be held in a defense means to close observing internal data and an internal processing procedure from the outside if at least. Moreover, the storage means of the above 2nd and the above-mentioned certification data generation means may be made to be constituted as a portable small arithmetic unit of an IC card etc. at least.

[0026] The above-mentioned certification data generation means consists of the 1st operation means and the 2nd operation means. Moreover, the 1st operation means Predetermined count is performed to a user's proper information memorized by the storage means of the above 2nd, and the auxiliary information for certification memorized by the storage means of the above 3rd. The description information on the above-mentioned access rating authentication is computed as the result. The 2nd operation means Predetermined count is performed to the data for authentication memorized by the storage means of the above 1st, and the description information on the access rating authentication computed by the 1st operation means, and the above-mentioned certification data can be generated as the result.

[0027] The above-mentioned certification data generation means consists of the 3rd operation means, the 4th operation means, and the 5th operation means. Moreover, the 3rd operation means Predetermined count is performed to the data for authentication memorized by the storage means of the above 1st, and the auxiliary information for certification memorized by the storage means of the above 3rd. The 4th operation means The count result perform predetermined count to the data for authentication memorized

by the storage means of the above 1st, and a user's proper information memorized by the 2nd storage means, and according [the 5th operation means] to the operation means of the above 3rd, Predetermined count is performed to the count result by the operation means of the above 4th, and the above-mentioned certification data can be generated as the result. Also in this case, the storage means of the above 2nd and the operation means of the above 4th may be made to be held in a defense means to close observing internal data and an internal processing procedure from the outside if at least. Moreover, the storage means of the above 2nd and the operation means of the above 4th can be constituted as a portable small arithmetic unit of an IC card etc. at least. In the embodiment as which a means to hold in a defense means can be made small-scale with this configuration, and the small configuration especially using IC chip etc. is required, it is effective.

[0028] Moreover, the description information on the above-mentioned access rating authentication is a decode key in a code function, and the above-mentioned data for authentication encipher suitable data using the encryption key corresponding to said decode key, and you may make it the above-mentioned certification data-verification means verify that the above-mentioned certification data which the above-mentioned certification data generation means generates decode the data for authentication correctly.

[0029] Moreover, you may make it verify that the above-mentioned certification data which the description information on the above-mentioned access rating authentication is an encryption key in a code function, and the above-mentioned certification data generation means generates encipher the above-mentioned data for authentication correctly using said encryption key.

[0030] Moreover, you may make it verify that the above-mentioned certification data which the description information on the above-mentioned access rating authentication is a signature key in a digital signature function, and the above-mentioned certification data generation means generates are the digital signature correctly generated to the above-mentioned data for authentication using said signature key.

[0031] Moreover, an encryption function may be an unsymmetrical key code function, and the description information on access rating authentication may be one side of a key.

[0032] Moreover, an encryption function may be a public-key-encryption function, and the description information on access rating authentication may be a private key.

[0033] Moreover, an encryption function may be a symmetry key code function, and the description information on access rating authentication may be a common private key.

[0034] Moreover, the storage means of the above 1st, the storage means of the above 2nd,

and the storage means of the above 3rd, The certification data generation equipment which consists of above-mentioned certification data generation means, and the 4th storage means which memorizes the data for authentication in addition to the above-mentioned certification data verification means, In the access rating authentication equipment with which certification data verification equipment equipped with the 5th storage means which memorizes certification data attests a user's access rating by communicating mutually Certification data verification equipment writes out the data for authentication memorized by the 4th storage means to the 1st storage means of certification data generation equipment. Certification data generation equipment The certification data generated based on the above-mentioned data for authentication written in the 1st storage means by the certification data generation means It writes out to the 5th storage means in certification data verification equipment, and certification data verification equipment can attest a user's access rating using the above-mentioned certification data written in the 5th storage means.

[0035] Moreover, the description information on the above-mentioned access rating authentication is the encryption key of an encryption function. Certification data verification equipment is equipped with a random-number generation means, and a random-number generation means is written in the 4th storage means by using the generated random number as the data for authentication. A certification data verification means You may make it verify enciphering the data for authentication whose certification data written in the 5th storage means by certification data generation equipment are said random number with the encryption key which is the description information on access rating authentication.

[0036] The description information on access rating authentication is the decode key of an encryption function. Certification data verification equipment Moreover, a random-number generation means, While it has the 6th storage means which memorizes the generated random number, and the 7th storage means which memorizes the ** data for authentication and a random-number generation means writes the generated random number in the 6th storage means After giving the random-number effectiveness which used said random number for the ** data for authentication memorized by the 7th storage means, it writes in the 4th storage means as data for authentication. A certification data verification means The result of having removed the random-number effectiveness by the random number memorized by the 6th storage means from the certification data in which it was written by the 5th storage means with the above-mentioned certification data generation equipment You may make it verify

decoding the ** data for authentication memorized by the 7th storage means with the decode key which is the description information on access rating authentication.

[0037] Moreover, the description information on the above-mentioned access rating authentication is the signature key of a digital signature function. Certification data verification equipment is equipped with a random-number generation means, and a random-number generation means is written in the 4th storage means by using the generated random number as the data for authentication. A certification data verification means You may make it verify that the certification data written in the 5th storage means by certification data generation equipment are a digital signature with the signature key it is [key] the description information on access rating authentication to the data for authentication which are said random number.

[0038] It is the RSA public key encryption under n, the description information on access rating authentication is a private key D, and the public key corresponding to a private key D is E. moreover, an encryption function -- law -- a certification data verification means the data C for authentication remembered to be the result of having squared the certification data R written in the 5th storage means E by the 4th storage means -- law -- you may make it verify a congruent thing (RE mod n = C mod n) under n

[0039] It is the RSA public key encryption under n, and the description information on access rating authentication is a private key D. moreover, an encryption function -- law -- It is squared several K' (=KE mod n) E under n. the ** data for authentication which the public key corresponding to a private key D is E, and are memorized by the storage means of the above 7th -- Data K -- law -- the random number r which generated the above-mentioned random-number generation means -- law -- with the number squared E under n It writes in said 4th storage means by using as the data for authentication several C (=rEK'mod n) by which it multiplied under n. said K' -- law -- a certification data verification means the law of the random number r memorized by the 6th storage means -- with the number which multiplied the certification data R in which it was written by the 5th storage means with certification data generation equipment by the inverse number under n You may make it verify that said K is congruent under Law n (K mod n=r-1R mod n).

[0040] It is the RSA public key encryption under n, and the description information on access rating authentication is a private key D. moreover, an encryption function -- law -- The auxiliary information t for certification which the public key corresponding to a private key D is E, and is memorized by the storage means of the above 3rd A user's proper information e memorized by the storage means of the above 2nd is subtracted from said D. It is data (t=D-e+omegaphi (n)) which add a product with Euler number [of

the un-colliding nature function values omega (=G (n, e)) and n] phi (n) depending on said n and e, and are obtained. The above-mentioned certification data generation means Furthermore, said t, the law from the data C for authentication written in said e and the 1st storage means -- you may make it generate said certification data by calculating the Dth power (CD mod n) of C under n

[0041] The above-mentioned certification data generation means consists of the 3rd operation means, the 4th operation means, and the 5th operation means. Moreover, the 3rd operation means Said t-th power (Ct mod n) of said C is calculated under the describing [above] method n. The 4th operation means You may make it the 5th operation means generate the certification data R (=CtCe mod n) by multiplying by the count result of the 1st and 2nd operation means under the describing [above] method n by calculating said e-th power (Ce mod n) of said C under the describing [above] method n. Also in this case, said 2nd storage means and said 4th operation means may be made to be built in in a defense means to defend an internal processing procedure and data from external observation.

[0042] It is the RSA public key encryption under n, and the description information on access rating authentication is a private key D. moreover, an encryption function -- law -- The auxiliary information t for certification which the public key corresponding to a private key D is E, and is memorized by the storage means of the above 3rd It is data (t=D+F (n, e)) which add the un-colliding nature function value F depending on proper information e and said law n of the user memorized by the storage means of the above 2nd (n, e) to said D, and are obtained. The above-mentioned certification data generation means Said t, the law from the data C for authentication written in said e and said 1st storage means -- you may make it generate said certification data by calculating the Dth power (CD mod n) of C under n

[0043] The above-mentioned certification data generation means consists of the 3rd operation means, the 4th operation means, and the 5th operation means. Moreover, the 3rd operation means Said t-th power (Ct mod n) of said C is calculated under the describing [above] method n. The 4th operation means Said F (n, e) ** (CF(n, e) mod n) of said C is calculated under the describing [above] method n. The 5th operation means You may make it generate the certification data R (=CtC-F(n, e) mod n) under the describing [above] method n by multiplying by the inverse number of the count result of the 3rd operation means, and the count result of the 4th operation means.

[0044] Moreover, said 2nd storage means and said 4th operation means may be made to be built in in a defense means to defend an internal processing procedure and data from external observation.

[0045] It is a Pohlig-Hellman unsymmetrical key code under p. moreover, an encryption function -- law -- The description information on access rating authentication is one key D, and the key of another side corresponding to Key D is E (DE mod p-1 = 1). A certification data verification means the data C for authentication remembered to be the result of having squared the certification data R written in the 5th storage means E by the 4th storage means -- law -- you may make it verify a congruent thing (RE mod p = C mod p) under p

[0046] It is a Pohlig-Hellman unsymmetrical key code under p. moreover, an encryption function -- law -- The description information on access rating authentication is one key D, and the key of another side corresponding to Key D is E (DE mod p-1 = 1). It is squared several K' (=KE mod p) E under p. the ** data for authentication memorized by the storage means of the above 7th -- Data K -- law -- the above-mentioned random-number generation means It writes in said 4th storage means by using as the data for authentication several C (=rEK' mod p) by which it multiplied under p. the generated random number r -- law -- the number squared E under p, and said K' -- law -- the law of the random number r with which the certification data verification means is memorized by the 6th storage means -- with the number which multiplied the certification data R in which it was written by the 5th storage means with certification data generation equipment by the inverse number under p You may make it verify that said K is congruent under Law p (K mod p=r-1R mod p).

[0047] It is a Pohlig-Hellman unsymmetrical key code under p. moreover, an encryption function -- law -- The description information on access rating authentication is one key D, and the key of another side corresponding to Key D is E (DE mod p-1 = 1). It is data (t=D+F (p, e)) with which the auxiliary information t for certification memorized by the storage means of the above 3rd adds the un-colliding nature function value F depending on the user proper information e memorized by the storage means of the above 2nd, and said p (p, e) to said D, and is acquired. The above-mentioned certification data generation means Said t, the law from the data C for authentication written in said e and the 1st storage means -- you may make it generate said certification data by calculating the Dth power (CD mod p) of C under p

[0048] The above-mentioned certification data generation means consists of the 3rd operation means, the 4th operation means, and the 5th operation means. Moreover, the 3rd operation means Said t-th power (Ct mod p) of said C is calculated under the describing [above] method p. The 4th operation means Under the describing [above] method p, the exponentiation (CF(p, e) mod p) of said C is calculated by making said F (p, e) into a characteristic. The 5th operation means You may make it generate the

certification data R (=CtC-F(p, e) mod p) under the describing [above] method p by multiplying by the inverse number of the count result of the 3rd operation means, and the count result of the 4th operation means. Also in this case, said 2nd storage means and said 4th operation means may be made to be built in in a defense means to defend an internal computational procedure and data from external observation.

[0049] Moreover, encryption functions are Law p and the ElGamal public key encryption under Generator a. The description information on access rating authentication is one key X, and the public key corresponding to Key X is Y (Y = aX mod p). u -- Above a -- law -- the number which made the suitable random number z the characteristic and carried out the exponentiation under p -- it is (u=az mod p) -- K' -- Above Y -- law -- with the number which made the above-mentioned random number z the characteristic, and carried out the exponentiation under p When it is a product with Data K (K'=YzK mod p), the group of u and K' is memorized by the storage means of the above 7th as ** data for authentication. The above-mentioned random-number generation means It writes in said 4th storage means by using as the data for authentication several C (=rK' modp) by which it multiplied under p. Above u and the generated random number r -- said K' -- law -- a certification data verification means the law of the random number r memorized by the 6th storage means -- with the number which multiplied the certification data R in which it was written by the 5th storage means with certification data generation equipment by the inverse number under p You may make it verify that said K is congruent under Law p (K mod p=r-1R mod p).

[0050] Moreover, encryption functions are Law p and the ElGamal public key encryption under Generator a. The description information on access rating authentication is one key X, and the public key corresponding to Key X is Y (Y = aX mod p). It is data (t=X+F (p, e)) with which the auxiliary information t for certification memorized by the storage means of the above 3rd adds the un-colliding nature function value F depending on the user proper information e memorized by the storage means of the above 2nd, and said p (p, e) to said X, and is acquired. The above-mentioned certification data generation means Said t, the law from the data u and C for authentication written in said e and the 1st storage means -- you may make it generate the above-mentioned certification data by calculating under p the number (Cu-X mod p) which broke C by the Xth power of Above u

[0051] The above-mentioned certification data generation means consists of the 3rd operation means, the 4th operation means, and the 5th operation means. Moreover, the 3rd operation means Said t-th power (ut mod p) of said u is calculated under the describing [above] method p. The 4th operation means Said F (p, e) ** (uF(p, e) mod n)

of said u is calculated under the describing [above] method p. The 5th operation means You may make it generate the certification data R (=Cu-tuF(p, e) mod p) by being as a result of [of the 3rd operation means] count, breaking Above C under the describing [above] method p, and multiplying by the count result of the 4th operation means further. In this case, said 2nd storage means and said 4th operation means may be made to be built in in a defense means to defend an internal computational procedure and data from external observation.

[0052] Moreover, a signature function is the ElGamal signature under Law p and Generator a. The description information on access rating authentication is one key X, and the public key corresponding to Key X is Y (Y = aX mod p). A certification data verification means the certification data R and S written in the 5th storage means -- receiving -- law -- under p the product of the value which made the characteristic the data C for authentication memorized by the 4th storage means in Above a, and carried out the exponentiation, and the value which squared Above Y R and the value which squared R S -- law -- you may make it verify a congruent thing (aC modp = YRRS mod p) under p

[0053] Moreover, a signature function is the ElGamal signature under Law p and Generator a. The description information on access rating authentication is one key X, and the public key corresponding to Key X is Y (Y = aX mod p). It is data (t=X+F (p, e)) with which the auxiliary information t for certification memorized by the storage means of the above 3rd adds the un-colliding nature function value F depending on the user proper information e memorized by the storage means of the above 2nd, and said p (p, e) to said X, and is acquired. The above-mentioned certification data generation means The k-th power of the above a under p is set to R (=akmod p). the certification data R and S -- generating -- hitting -- the suitable random number k -- generating -- law -- with said t You may make it calculate S (=(C-RX) k-1 mod p-1) by multiplying the number which lengthened the product of X and r from C by the inverse number of k under law p-1 from the data C for authentication written in said e and the 1st storage means. In this case, the 2nd storage means and a certification data generation means may be made to be built in in a defense means to defend an internal computational procedure and data from external observation.

[0054] Moreover, the above-mentioned user's proper information is the decode key of a code function, and when the auxiliary information for certification enciphers the description information for access rating authentication with the encryption key corresponding to said decode key and the 1st operation means decodes the auxiliary information for certification using the decode key which is the above-mentioned user's

proper information, the description information for access rating authentication may make compute. In this case, the above-mentioned code function may be an unsymmetrical key code function, and a user's proper information may be one key. Moreover, the above-mentioned code function may be a public-key-encryption function, and a user's proper information may be a private key. Moreover, an account code function may be a symmetry key code function, and a user's proper information may be a common private key.

[0055] Moreover, 8th storage means by which the above-mentioned certification data verification means memorizes the plaintext data corresponding to the enciphered above-mentioned data for authentication or the above-mentioned ** data for authentication which is data further, The result of having removed the random-number effectiveness from certification data if needed [that have a comparison means and the above-mentioned certification data generation means generated the above-mentioned comparison means / the above-mentioned certification data or if needed], The plaintext data memorized by the 8th storage means are compared, when both are in agreement, it restricts, and you may make it judge that the above-mentioned certification data are just.

[0056] Moreover, 9th storage means by which the above-mentioned certification data verification means memorizes the result of having given the predetermined one-way function to the plaintext data corresponding to the enciphered above-mentioned data for authentication or the above-mentioned ** data for authentication which is data, further, It has the 6th operation means and comparison means which performs a top Norikazu directional function. The 6th operation means If required for the above-mentioned certification data which the above-mentioned certification data generation means generated, after removing the random-number effectiveness, a one-way function is given. The above-mentioned comparison means The data remembered to be a count result by the 6th operation means by the 9th storage means are compared, when both are in agreement, it restricts, and you may make it judge that the above-mentioned certification data are just.

[0057] The above-mentioned certification data verification means includes a program execution means further. Moreover, the above-mentioned data for authentication, or the above-mentioned ** data for authentication It is data which encipher a program and are obtained. The above-mentioned certification data verification means If required in the above-mentioned certification data which the certification data generation means generated, after removing the random-number effectiveness, by handing over for a program execution means as a program It restricts, when the above-mentioned data for

authentication or the ** data for authentication with which the certification data generation means was enciphered and which is a program is decoded correctly (i.e., when the enciphered program is decoded correctly), and a program execution means may be made to perform right actuation.

[0058] Moreover, the program the above-mentioned certification data verification means is further remembered to be by the program store means including the program execution means, the program store means, and the program decode means The part or all is enciphered. The above-mentioned data for authentication, or the above-mentioned ** data for authentication It is data which encipher separately the decode key for decoding said enciphered program, and are obtained. The above-mentioned certification data verification means The above-mentioned certification data which the certification data generation means generated are handed over for a program decode means. A program decode means By using the certification data which said certification data generation means generated as a decode key, after removing the random-number effectiveness, if required By performing the program which decodes the required part of the program memorized by the program store means and by which the program execution means was decoded It restricts, when a certification data generation means is correctly decoded in the above-mentioned data for authentication, or the ** data for authentication (i.e., in order to decode the enciphered program when a decode key is decoded correctly), and a program execution means may be made to perform right actuation.

[0059] Moreover, the above-mentioned certification data generation equipment and the above-mentioned certification data authentication equipment are formed in the same housing, and the above-mentioned certification data generation equipment and the above-mentioned certification data authentication equipment may be made to communicate, without understanding the communication media of the exterior of the housing concerned.

[0060] Moreover, it sets to the access rating authentication approach which attests the above-mentioned user's access rating by verifying the justification of the certification data generated from the data for authentication in order to prove a user's access rating according to the 2nd side face of this invention. The step which memorizes the above-mentioned data for authentication, and the step which memorizes a user's proper information, The step which memorizes the auxiliary information for certification which it is as a result of activation that predetermined count was performed, to the above-mentioned user's proper information, and the description information on access rating authentication, The step which performs predetermined count to the

above-mentioned data for authentication, the above-mentioned user's proper information, and the above-mentioned auxiliary information for certification, and generates certification data, It is made to perform the step which verifies that the certification data generated by the above-mentioned certification data generation means are generated based on the description information on the above-mentioned access rating authentication.

[0061] Moreover, in order to attest the above-mentioned user's access rating by verifying the justification of the certification data generated from the data for authentication in order to prove a user's access rating according to the 3rd side face of this invention In the program product for access rating authentication used by computer The step which memorizes the above-mentioned data for authentication, and the step which memorizes a user's proper information, The step which memorizes the auxiliary information for certification which it is as a result of activation that predetermined count was performed, to the above-mentioned user's proper information, and the description information on access rating authentication, The step which performs predetermined count to the above-mentioned data for authentication, the above-mentioned user's proper information, and the above-mentioned auxiliary information for certification, and generates certification data, He is trying to use the step which verifies that the certification data generated by the above-mentioned certification data generation means are generated based on the description information on the above-mentioned access rating authentication for performing the above-mentioned computer.

[0062] Moreover, in order to generate the certification data which have justification verified in order to attest a user's access rating from the data for authentication according to the 4th side face of this invention In the program product for certification data generation used by computer The step which memorizes the above-mentioned data for authentication, and the step which memorizes the proper information on user **, The step which memorizes the auxiliary information for certification which it is as a result of activation that predetermined count was performed, to the above-mentioned user's proper information, and the description information on access rating authentication, He is trying to use the step which performs predetermined count to the above-mentioned data for authentication, the above-mentioned user's proper information, and the above-mentioned auxiliary information for certification, and generates certification data for performing the above-mentioned computer.

[0063] Moreover, the above-mentioned user's access rating is attested by verifying the justification of the certification data generated in order to prove a user's access rating according to the 5th side face of this invention. The 1st storage means which memorizes

the data for authentication to the program execution control device which controls program execution based on authentication of the above-mentioned rating, The 2nd storage means which memorizes a user's proper information, and the above-mentioned user's proper information, The 3rd storage means which memorizes the auxiliary information for certification which it is as a result of activation that predetermined count was performed, to the description information on access rating authentication, The above-mentioned user's proper information memorized by the storage means of the above 2nd and the above-mentioned auxiliary information for certification memorized by the storage means of the above 3rd are used. He is trying to establish a certification data generation means to generate the above-mentioned certification data from the above-mentioned data for authentication, a means to verify the justification of the certification data generated from the above-mentioned certification data generation means, and a means to continue program execution when the justification of the above-mentioned certification data is verified.

[0064] To moreover, the information processor which attests the above-mentioned user's access rating and permits access to the above-mentioned predetermined information processing resource by verifying the justification of the certification data generated in order to prove access rating of the user to a predetermined information processing resource according to the 6th side face of this invention The 1st storage means which memorizes the data for authentication, and the 2nd storage means which memorizes a user's proper information, The 3rd storage means which memorizes the auxiliary information for certification which it is as a result of activation that predetermined count was performed, to the above-mentioned user's proper information, and the description information on access rating authentication, The above-mentioned user's proper information memorized by the storage means of the above 2nd and the above-mentioned auxiliary information for certification memorized by the storage means of the above 3rd are used. A certification data generation means to generate the above-mentioned certification data from the above-mentioned data for authentication, a means to verify the justification of the certification data generated from the above-mentioned certification data generation means, and a means to grant a permission in access to the above-mentioned predetermined information processing resource based on verification of the above-mentioned justification are made to prepare.

[0065]

[The mode of implementation of invention] First, the theoretic example of a configuration of this invention is explained. The user authentication system of this example of a configuration is applicable not only to the execution control of application

but access controls, such as privacy protection and the file of e-mail, and a computer resource.

[0066] In drawing 1, the user authentication system consists of certification data verification equipment 10 and certification data generation equipment 11, and certification data generation equipment 11 receives the access ticket (auxiliary data for certification) 13 from access ticket generation equipment 12. Certification data verification equipment 10 performs the verification routine 15. Certification data generation equipment 11 holds the user proper information 16 and the access ticket 13, and performs the certification data generator 17.

[0067] Access ticket generation equipment 12 is prepared for an application implementer's etc. protection side, or the third person who can trust it. The access ticket 13 is generated based on the description information 14 and the user proper information 16 on access rating authentication, this access ticket 13 is sent to a user through sending of a communication link or a floppy diskette, and access ticket generation equipment 12 is held at a user's certification data generation equipment 11. Then, certification data verification equipment 10 sends out the data 18 for authentication to certification data generation equipment 11. Certification data generation equipment 11 generates the certification data 19 using the access ticket 13 and the user proper information 16, and answers certification data verification equipment 10 in this. Certification data verification equipment 10 verifies the justification of certification data based on the data for authentication. That is, it verifies that certification data are data generated based on the data for authentication, and the description information on access rating authentication.

[0068] If the justification of certification data is verified, a user's access rating will be attested and program execution continuation, access to a file, etc. will be allowed according to this.

[0069] The above configuration is further explained taking the case of the execution control of an application program.

[0070] In such a configuration, the user of an application program holds the user proper information 16 for even free first. User proper information is the important only information that it is equivalent to the password in password authentication, and a user's identity is proved. Since a user without the just right of use will also be allowed use of an application program etc. when a user can copy and distribute the user proper information 16, the user proper information 16 is protected by the defense means so that the user who is the just holder cannot steal this, either. The hardware (it is hereafter called tamper-proof hardware) which has the defense force to theft of the

internal state by the probe can constitute this defense means. About the implementation technique of tamper-proof hardware, it mentions later.

[0071] Moreover, in addition to the above-mentioned user proper information 16, the certification data generator 17 which performs predetermined count procedure is given to a user. This program 17 is for communicating with the user authentication routine in application (certification data verification routine 15), and if two parameters, the user proper information 16 and the access ticket 13, are given, it will generate the certification data 19 which calculate to the input value of arbitration and prove a user's identity. Although the user proper information 16 is used in process of this count, since there is a problem when the user proper information 16 is revealed outside for the reason explained above, a part of above-mentioned program [at least] needs to be protected by the above-mentioned defense means.

[0072] Suppose that the user proper information storage means protected by the above-mentioned defense means and a part of program, the equipment (for example, constituted by memory and MPU) for performing this program part, and the above-mentioned defense means are combined hereafter, and it is called a token (the sign 20 of drawing 1 shows). A token can also be considered as the configuration which has portability like an IC card.

[0073] On the other hand, into an application program, the certification data verification routine 15 is incorporated like the conventional execution control technique. The certification data verification routine 15 is the same as that of the conventional technique in the point created so that it may communicate with the above-mentioned certification data generator 17 which a user holds, a reply result (certification data 19) may restrict to a right case and it may continue program execution. Therefore, the programmer needs to learn how to calculate the combination of transmit data (data 18 for authentication), and the right reply data (certification data 19) to it.

[0074] Several operations of the certification data verification routine 15 are described below.

1. Into the certification data verification routine 15, the reply data (expected value) it is expected that are data (data 18 for authentication) which should be transmitted are embedded. The certification data verification routine 15 takes out the above-mentioned transmit data, transmits to a user, and receives a reply from a user. Subsequently, the reply data and the above-mentioned expected value from a user are compared, when both are in agreement, the next step of a program is performed, and program execution is stopped when not in agreement.

[0075] Here, in being as a result of the encryption to which reply data follow the

predetermined encryption algorithm of transmit data, the description information on access rating authentication serves as an encryption key.

[0076] 2. Into the certification data verification routine 15, the data which should be transmitted, and the data (expected value) which gave the one-way function to the reply data expected are embedded. The certification data verification routine 15 takes out the above-mentioned transmit data, transmits to a user, and receives a reply from a user. Subsequently, when both are in agreement with reply data from a user in the value which gave the top Norikazu directional function as compared with the above-mentioned expected value, the next step of a program is performed, and program execution is stopped when not in agreement.

[0077] Here, in being as a result of the encryption to which reply data follow the predetermined encryption algorithm of transmit data, the description information on access rating authentication serves as an encryption key.

[0078] 3. Give the protection it is made to become impossible [this program execution] by enciphering according to the encryption algorithm which was able to define a part of code of an application program beforehand. The certification data verification routine 15 transmits the code by which encryption was carried out [above-mentioned] to a user, and performs procedure which replaces with the code before encryption the value received as the reply.

[0079] According to the above configuration, it restricts, when it is right decode of the code as which reply data were enciphered, and this program execution becomes possible. The description information on the access rating authentication in this case serves as a decode key for decoding the enciphered code.

[0080] 4. Give the protection it is made to become impossible [this program execution] by enciphering according to the encryption algorithm which was able to define a part of code of an application program beforehand. Furthermore, it embeds into the certification data verification routine 15 by using as transmit data the data which enciphered separately the encryption key used for encryption of the above-mentioned code, and the decode key which makes a pair. The certification data verification routine 15 transmits the decode key by which encryption was carried out [above-mentioned] to a user, and decodes the code by which encryption was carried out [above-mentioned] by using as a decode key the value received as the reply.

[0081] According to the above configuration, when reply data are the decode key decoded correctly, the code by which encryption of the hook was carried out [above-mentioned] is decoded correctly, and this program execution of it becomes possible. The description information on the access rating authentication in this case

serves as a decode key for decoding the enciphered decode key.

[0082] Now, with the conventional execution control technique, user proper information (a user's authentication key) is the same as the description information on access rating authentication. The conventional certification data generating routine calculates reply data by considering as an input the description information on access rating authentication, and the data transmitted from the certification data verification routine.

[0083] On the other hand, the user proper information 16 and the description information 14 on access rating authentication have the description of this invention in a mutually-independent point. the data (data 18 for authentication) with which the certification data generator 17 was transmitted from the user proper information 16 and the certification data verification routine 15 also in this example of a configuration -- in addition, reply data (certification data 19) are calculated by considering the access ticket 13 as an input. This configuration has the following properties.

[0084] 1. The access ticket 13 is data calculated based on the specific user proper information 16 and the description information 14 on access rating authentication.

2. It is impossible in computational complexity at least to calculate the description information 14 on access rating authentication for the user proper information 16 from the access ticket 13 to not knowing.

3. The certification data generator 17 calculates right reply data only within the case where the right combination of the user proper information 16 and the access ticket 13, i.e., the combination of the access ticket 13 calculated based on the user proper information 16 and this user proper information 16, is inputted.

[0085] By the above, a programmer can perform execution control by a user possessing the user proper information 16 beforehand by creating an application program independently [the user proper information 16 which a user possesses], creating the access ticket 13 according to the user proper information 16 and the description information 14 on access rating authentication used for creation of an application program, and distributing.

[0086] Moreover, the proper information which shall consist of two proper information and uses the user proper information 16 on the occasion of creation of the access ticket 13, and the proper information which a user uses in a communications program can also be distinguished and used. The most typical example is the approach of making user proper information 16 a public key pair, and exhibiting a public key, using for access ticket creation, and enclosing the individual key into the token 20 as a user individual's confidential information. In this case, it becomes possible by enabling it to calculate the access ticket 13 from the description information 14 on access rating authentication,

and the public key of the above-mentioned public key pair to calculate the access ticket 13, keeping the user proper information 16 secret.

[0087]

[Example] It is based on an example about a concrete configuration by the next, and explains.

[Whole configuration]

[0088] Before describing the example according to concrete individual, the overview of the operation gestalt of this invention is described below.

[0089] First, the case where this invention is used for the execution control of the application program which operates on a user's PC or a workstation is described. Drawing 2 shows the whole equipment configuration in this operation gestalt. In addition, in drawing 2 R> 2, the sign corresponding to a corresponding part is attached with drawing 1 , and detailed explanation is not repeated.

[0090] In this operation gestalt, certification data generation equipment 11 is realizable as a program 32 for certification on the computer 31 which a user uses. Under the present circumstances, in order to raise the safety of the proper information (user proper information) for identifying a user, it is also possible to use together the hardware 33 for certification (an IC card, board, etc.) with which this computer 31 is equipped and which has a tamper-proof property. Under the present circumstances, if hardware with portability like an IC card is used, it is convenient when a user works on two or more PCs or a workstation.

[0091] Certification data verification equipment 10 is constituted as a part of application program 34 which this user uses. That is, if a user starts this application program 34 on PC or a workstation, the certification data verification equipment 10 described as a program in this application program 34 is started, it will communicate with certification data generation equipment 11, user authentication will be performed, and activation of this application program will be enabled only within the case where a communication link is completed correctly.

[0092] In order for a user to use said application program 34 with which certification data verification equipment 10 was embedded, it is published by user him and it is necessary to acquire the auxiliary information for certification corresponding to said application program (access ticket). When user proper information is enclosed with the IC card, a user equips said PC or workstation with an IC card, for example, while registering the acquired access ticket into the program 32 for certification installed on said PC or the workstation.

[0093] Certification data generation equipment 11 (constituted by the program and IC

card on PC or a workstation) calculates based on user proper information and an access ticket, and performs a communication link with certification data verification equipment 10 based on the count.

[0094] As a result of a communication link, when user proper information, the access ticket, and said application program 34 with which certification data verification equipment 10 was embedded correspond surely [three], it restricts that authentication by certification data verification equipment 10 is successful.

[0095] Authentication is not successful when either user proper information or an access ticket is missing.

[0096] An access ticket is published by specific addressing to a user. That is, a specific user's user proper information is used on the occasion of generation of an access ticket. When the user proper information used for an access ticket generate time and said user proper information used by certification data generation equipment 11 are not in agreement, authentication is not successful too.

[0097] Moreover, an access ticket is generated based on the description information on specific access rating authentication, and certification data verification equipment 10 is constituted so that the description information on this access rating authentication may be attested. Therefore, authentication is not successful also when the description information used as the basis of generation of an access ticket and the description information which the certification data verification equipment 10 currently embedded at the application program 34 tends to attest do not correspond mutually.

[0098] In addition, in drawing 2 , 35 is control programs, such as an operating system, and 36 shows hardware at large.

[0099] Moreover, it is good also as that with which it performs on another computer by which the application program 34 was combined by the network, and an activation result communicates to the computer which a user uses through a network. In this case, it becomes a configuration based on the so-called server client model. In the case of execution control of the application program performed on a user's PC described previously or a workstation, when a server client model is followed to the communication link with certification data generation equipment 11 and certification data verification equipment 10 being performed as the so-called interprocess communication, the communication link with certification data generation equipment 11 and certification data-verification equipment 10 is performed as a communication link according to network protocols, such as TCP/IP.

[0100] Moreover, also when the application program is constituted on the dedicated device, it is possible to apply this invention. For example, the whole certification data

generation equipment shall be mounted in an IC card, and the acquired access ticket shall also be registered into an IC card. Although certification data verification equipment is mounted on said dedicated device, this dedicated device is equipped with the slot for inserting an IC card, and a user attests by inserting the IC card owned into this slot. The configuration by such dedicated device is applicable to the ATM machine of a bank, the game machine in a game center, etc.

[0101] About acquisition of the access ticket by the user, there are an approach of a common pin center,large generating according to the issue request from a user, and distributing and an approach which the implementer of an application program borrows the assistance of an access ticket issue program or access ticket generation equipment, and generates according to an individual.

[0102] Although it is good also as what is delivered by the user through portable mold storages, such as a floppy disk, since the access ticket is equipped with sufficient safety, the generated access ticket may be constituted so that it may be delivered through a network using an electronic mail etc.

[0103] The safeties of an access ticket are the following two properties.

[0104] the user by whom an access ticket is a registered form, namely, the access ticket was published -- only he (holder of the user proper information that it was correctly used for the access ticket generate time) can operate certification data generation equipment correctly using this access ticket. Therefore, even if a holder in bad faith intercepts a network and gets other users' access ticket unjustly, unless this third person gets the user proper information of the user of the normal which is the issue place of an access ticket, it is impossible to use this access ticket.

[0105] The access ticket holds still stricter safety. That is, even if a holder in bad faith collects the access tickets of the arbitration number and performs what kind of analysis, it is impossible to constitute equipment which another access ticket is forged [equipment] based on the acquired information, or actuation of certification data generation equipment is copied [equipment], and forms authentication.

[0106] Below, it is based on an example and a more concrete configuration is explained.

[The first example]

[0107] In the first example in this invention, the access ticket t is data generated based on the following formula 1.

[Equation 1] (1) t = D-e+omegaphi (n)

Each notation in an upper type expresses the following.

[0108] n is the product of the number p and q of the RSA methods, i.e., the two sufficiently big prime factors, (n=pq).

[0109] phi (n) is the Euler number of n, i.e., the product of p-1 and q-1, (phi (n) = (p-1) (q-1)).

[0110] The user proper information e is a different number for every user, and it is used in order to identify a user.

[0111] the access ticket private key D -- law -- it is a RSA private key under a number n, and a formula 2 is filled.

[Equation 2] (2) gcd(D, phi (n)) =1 -- here, gcd (x y) expresses the greatest common measure of more than 2 [x] and y. The property expressed by the formula (2) guarantees that several E which fills a formula 3 exists.

[Equation 3]

(3) ED mod phi (n) = 1E is called an access ticket public key.

[0112] omega is a number which becomes settled depending on n and e, and when n differs either from e, its value of the corresponds easily, twists it (it does not collide), and it is defined like. There is also a method of omega setting and defining omega like a formula 4 as an example of the direction using one-way hash function h.

[Equation 4] (4) Omega=h (n | e)

However, notation | expresses junction of a bit string.

[0113] One-way hash functions are x which fills h(x) =h (y) and which is different from each other, and a function in which computing y has the property in which it is remarkable and difficult. As an example of an one-way hash function, it is RSA. Data Security The specification SHS (Secure Hash Standard) by MD2 and MD4 by Inc., MD5, and the U.S. federal government is known.

[0114] In the number which appeared during the above-mentioned explanation, t, E, and n can be exhibited and D, e, omega, p, remaining q, and remaining phi (n) need to be secret in addition to those who have the right which creates a ticket. With reference to drawing, the first example is further explained to a detail. Drawing 3 shows the configuration of the first example in this invention, and drawing 4 shows the flow of the data in drawing 3 . In drawing 3, certification data verification equipment 10 is constituted including the access ticket public key storage section 101, the random-number-generation section 102, the random-number storage section 103, the received-data storage section 105, the verification section 106, the activation section 107, and the error-processing section 108. Moreover, certification data generation equipment 11 is constituted including the received-data storage section 111, the 1st operation part 112, the access ticket storage section 113, the 2nd operation part 114, the user proper information storage section 115, and the certification data generation section 116.

[0115] Actuation is explained below.

1. When a user accesses, certification data verification equipment 101 is started. The following gestalten can be considered about starting of certification data verification equipment 10.

[0116] When certification data verification equipment 10 is constituted as a part of application program which operates on a user's PC or a workstation, a user starts this application program by the usual approach using designating devices, such as a keyboard or a mouse. Certification data verification equipment 10 is started by things by reaching the program whose activation of an application program constitutes certification data verification equipment 10.

[0117] certification data verification equipment 10 constitutes on other PCs tied with the network, or a workstation (it is called a server) -- having -- **** -- a case -- a user -- oneself -- when the communications program on PC or a workstation is started and this communications program performs a communicative open request to said server according to a predetermined procedure, certification data verification equipment 10 is started. For example, in case a user's communications program communicates with a server, supposing it follows the procedure called TCP/IP, it will enable the demon (inetd) on a server to start certification data verification equipment 10 according to a TCP connection request by matching certification data verification equipment with the specific port of a server beforehand, and setting up so that a user's communications program may specify this port further and a TCP connection request may be required of a server. Such an implementation approach is widely used in networks, such as the Internet.

[0118] It is also possible to use certification data verification equipment 10 as the equipment of the exclusive purpose. For example, certification data verification equipment 10 can be constituted as a program written in the program or EEPROM which was able to be burned on ROM in an IC card reader writer, and certification data generation equipment 11 can be considered as the program mounted in the microcontroller of an IC card. In this case, when a user inserts an IC card in a reader writer, certification data verification equipment 10 is started.

[0119] 2. the law of the RSA cryptograph certification data verification equipment 10 is remembered to be by the data C for authentication, and the access ticket public key storage section 101 -- although a number n is written in the received-data storage section 111 in certification data generation equipment 11, this data C for authentication is generated by the following approaches.

[0120] By the random-number-generation section 102 in certification data verification equipment, a random number r is generated so that it may become the number n of the

RSA methods and relatively prime which are held at the access ticket public key storage section 101, and it records on the random-number storage section 103. Furthermore, let this random number r be the data C for authentication. the certification data which certification data generation equipment 11 returns in this case so that it may mention later -- C -- law -- it becomes what was enciphered using RSA cryptograph also as ** of a number n.

[0121] Since the value of C is the random-number r itself, it turns into a different value at every communication link, and has the effectiveness of preventing a replay attack.

[0122] 3. the RSA method which the 1st operation part 112 in certification data generation equipment 11 acquired the access ticket t memorized by the access ticket storage section 113, and was written in the received-data storage section 111 -- it is a several n basis, and perform a formula 5 and obtain middle information R'.

[Equation 5] (5) R'=Ct mod n [0123] 4. a user's proper information e that the 2nd operation part 114 in certification data generation equipment 11 is memorized by the user proper information storage section 115 -- acquiring -- count of a formula 6 -- performing -- difference -- acquire Information S.

[Equation 6] (6) S=Ce mod The certification data generation section 116 in n5. certification data generation equipment 11 obtains R' and S from the 1st and 2nd operation part 112 and 114, calculates a formula 7 and obtains R.

[Equation 7] (7) R=R'S mod n [0124] 6. Certification data generation equipment 11 returns R to the received-data storage section 105 of certification data verification equipment 10.

[0125] 7. the open characteristic E and the RSA method the verification section 106 in certification data verification equipment 10 is held first at the certification data R returned to the received-data storage section 105, and the access ticket public key storage section 101 -- calculate a formula 8 based on several n.

[Equation 8] (8) RE mod It confirms that a formula 9 is realized by n Ranking second and comparing with this count result the random number C (=r) currently held in the random-number storage section 103.

[Equation 9]

(9) C mod n = RE mod When n type (9) is materialized, the activation section 107 is started, processing is continued, when not materialized, the error-processing section 108 is started and error processing is performed.

[0126] [the second example] -- the configuration of the access ticket t in the second example of this invention and the operation of certification data certification equipment are the same as that of it in said first example. The data for authentication which

certification data verification equipment 10 generates in the second example to certification data having been a data encryption for authentication in the first example are encryption (with the random-number effectiveness) of certification data, and certification data generation equipment 11 decodes the data for authentication, and generates certification (have maintained random-number effectiveness) data. With reference to drawing, the second example is further explained to a detail. Drawing 5 shows the configuration of the second example in this invention, and drawing 6 shows the flow of the data in drawing 5 . In drawing 5, certification data verification equipment 10 is constituted including the access ticket public key storage section 101, the random-number-generation section 102, the random-number storage section 103, the received-data storage section 105, the random-number-ized section 121, the ** data storage section 122 for authentication, the random-number effectiveness removal section 123, and the activation means 310. Moreover, certification data generation equipment 11 is constituted including the received-data storage section 111, the 1st operation part 112, the access ticket storage section 113, the 2nd operation part 114, the user proper information storage section 115, and the certification data generation section 116.

[0127] Actuation is explained below.

1. When a user accesses, certification data verification equipment 10 is started.

[0128] It is not different from the case of the first example for the server program on the server connected through PC, workstation, and network of the application program and user who operate on a user's PC or a workstation or all of the equipment of dedication like an IC card reader writer to be possible as the implementation approach of certification data verification equipment.

[0129] 2. the law of the RSA cryptograph by which certification data verification equipment 10 is held at the data C for authentication, and the access ticket public key storage section 101 -- although a group with a number n is written in the received-data storage section 111 in certification data generation equipment 11, the data C for authentication are generated by the following approaches.

[0130] By the random-number-generation section 102 in certification data verification equipment, a random number r is generated so that it may become the number n of the RSA methods and relatively prime which are held at the access ticket public key storage section 101, and it records on the random-number storage section 103. the open characteristic E as which the random-number-ized section 121 is stored in the access ticket public key storage section 101, and law -- a formula 10 is calculated by acquiring a number n and acquiring data C' further memorized by the ** data storage section 122

for authentication.

[Equation 10] (10) C=rEC' mod n -- here, ** data C' for authentication is the value which was generated so that relational expression 11 might be filled to Data K, and was stored in the ** data storage section 122 for authentication.

[Equation 11] (11) C'=KE mod n -- here, if certification data verification equipment 10 is constituted so that Data K may not be held to certification data verification equipment but only C' which it is as a result of the encryption may be held instead, risk of Data K being revealed from certification data verification equipment 10 is avoidable.

[0131] if it sees fundamentally -- the data C for authentication -- law -- the basis of a number n -- RSA cryptograph -- using -- Data K -- enciphering -- certification data generation equipment 11 -- C -- law -- Data K are reproduced by decoding using RSA cryptograph under a number n. However, since it always becomes the same thing and the so-called replay attack becomes possible, the communication link between certification data verification equipment 10 and certification data generation equipment 11 gives the random-number effectiveness to the data for authentication using a random number r, and in case it verifies the data which certification data generation equipment 11 returns, it consists of as [this] so that the random-number effectiveness may be removed.

[0132] 3. the RSA method which the 1st operation part 112 in certification data generation equipment 11 acquired the access ticket t memorized by the access ticket storage section 113, and was written in the received-data storage section 111 -- perform a formula 12 by the several n basis, and obtain middle information R'.

[Equation 12] (12) R'=Ct mod n [0133] 4. a user's proper information e that the 2nd operation part 114 in certification data generation equipment 11 is memorized by the user proper information storage section 115 -- acquiring -- count of a formula 13 -- performing -- difference -- acquire Information S.

[Equation 13] (13) S=Ce mod The certification data generation section 116 in n5. certification data generation equipment 11 obtains R' and S from the 1st and 2nd operation part 112 and 114, calculates a formula 14 and obtains R.

[Equation 14] (14) R=R'S mod n [0134] 6. Certification data generation equipment 11 returns R to the received-data storage section 105 of certification data verification equipment 10.

[0135] 7. The random-number effectiveness removal section 123 in certification data verification equipment 10 takes out the certification data R from the random number r previously generated out of the random-number storage section 103, and the received-data storage section 106, and calculates a formula 15.

[Equation 15] (15) K' -- the combination of the proper information e of the access ticket t used in =r-1R mod n certification data generation equipment 11, and a user -- a right case -- as long as -- note that K' obtained as a result of count and K are in agreement.

[0136] Although calculated K' is handed over by the activation means 310 in certification data verification equipment 10, the activation means 310 is constituted so that it may restrict when K'=K is materialized, and processing of normal may be performed.

[0137] Below, several construction of the activation means 310 in certification data verification equipment 10 is described.

[0138] 1. Memorize Data K beforehand to storage section 310a in the example activation means 310 of a configuration of drawing 7. Comparator 310b in the activation section 310 compares directly K' which removes the random-number effectiveness and is obtained from the certification data R sent from this K and certification data generation equipment 11, when K'=K is materialized, it restricts it, it performs processing of normal, and when not materialized, error processing of stopping processing is performed (drawing 8).

[0139] There is a weak spot on the insurance that the data K used for verification appear in equipment in this example of a configuration. For example, it is not necessarily impossible to analyze a program and to steal K, when constituted as certification data verification equipment 10 and a program to which the activation means 310 operates on a user's PC or a workstation especially, even if difficult. The value of K serves as a place which a user gets to know, and becomes possible [constituting the equipment which copies / that the random number generated with certification data verification equipment can be expected further and / actuation of certification data generation equipment], and unlawful access of it by spoofing is attained.

[0140] 2. Since the fault of the example above of a configuration of drawing 9 is improved, the data memorized by storage section 310a can also be set to data h (K) obtained by not the K itself but K by giving the above-mentioned one-way hash function h. It is remarkably difficult to compute x which fills y=h (x) from the data y memorized by storage section 310a from the property of an one-way hash function.

[0141] The activation section 310 has transducer 310c which returns the result of having given the one-way hash function to the input data. Comparator 310b compares the data (=h (K)) memorized by the output h of the above-mentioned transducer 310c (K'), and storage section 310a (drawing 10).

[0142] In this example of an approach, since it is remarkably difficult to calculate h (K)

to K which the data K used for verification did not appear in the program, and was memorized by storage section 310a, it can be said that it is safer than the example of drawing 7 .

[0143] Program execution is controlled by this configuration to be shown in drawing 10 .

[0144] However, in the program, comparator 310b is constituted as conditional statement, when it is certification data verification equipment 10 and the program to which the activation means 310 operates on a user's PC or a workstation especially, with a configuration for which analysis and an alteration of a program are comparatively easy, is the point which can alter a program so that this conditional statement may be skipped, and, in addition, has the weak spot.

[0145] 3. Hold in the ** data storage section 122 for authentication in the example of a configuration of the example 3rd of a configuration of drawing 11 , using as ** data Cfor authentication' the data which enciphered a part or all of a program of a code. [of certification data verification equipment 10] [of the activation section 310] That is, K is a part or all of a code of an activation section program.

[0146] The activation means 310 embeds data K' which removes the random-number effectiveness and is obtained from the reply data from certification data generation equipment 11 in the location where it was beforehand set in the program. That is, the activation means 310 has 310d of code storage sections which memorize data K' as a code, code incorporation section 310e which incorporates this code in a program, and 310f of code activation sections which perform a program. When certification data generation equipment 11 answers a letter in right data, activation of a program is attained only within the case where it is K'=K (drawing 12).

[0147] Unjust activation can be prevented even when [with comparatively low safety] the activation means 310 consists of this example of a configuration as an application program which operates on a user's PC or a workstation, since a part or all of a code indispensable to program execution is enciphered.

[0148] The case where the activation means 310 is constituted as an application program which operates on a user's PC or a workstation is taken for an example, and a still more detailed configuration is described.

[0149] 310d of code storage sections in which certification data are written is the storage region where it was specified in the computer.

[0150] 310f of code activation sections is CPU and OS of a computer. CPU and OS cooperate and execute in order the run command memorized to the program field of a computer. A series of run commands which offer a specific function are called a program code.

[0151] The stereo of code incorporation section 310e is a program code first performed in the activation means 310. Code incorporation section 310e can direct the address of 310d of code storage sections in 310f of code activation sections directly and indirectly. For example, code incorporation section 310e may direct the physical address of 310d of code storage sections in 310f of direct-code activation sections, when OS of a computer performs virtual addressing, code incorporation section 310e may direct the virtual address of 310d of code storage sections, and the approach of changing into a physical address the virtual address received via CPU is sufficient as OS.

[0152] If code incorporation section 310e which is a program is started where certification data are written in 310d of code storage sections, it will order 310f of code activation sections, and code incorporation section 310e will perform them so that the contents memorized to the address of 310d of code storage sections may be written out to the specific address of the program field on a computer.

[0153] Subsequently, code incorporation section 310e orders 310f of code activation sections using a JMP instruction etc. to execute the run command of the specific address in a program field to which ordered 310f of code activation sections, and the contents of storage of 310d of code storage sections were made to write out.

[0154] In this example of a configuration, if certification data are correctly generated by certification data generation equipment 11, data after removing the random-number effectiveness will be a series of run commands 310f of program codes, i.e., the code activation section. Therefore, with the above-mentioned configuration, the program code decoded by the certification data generation means 11 will be performed following on the program code of code incorporation section 310e.

[0155] 4. In the example of a configuration of the example 3rd of a configuration of drawing 13, a decode key required in order to decode the enciphered code can also be set to K. According to this configuration, it cannot be concerned with the size of the code to encipher, but it can become possible to hold down the size of K, i.e., the size of ** data C' for authentication, to a small fixed value, and a communicative overhead can be decreased.

[0156] The activation section 310 decodes the code of the field where it was beforehand set in the program using data K' which removes the random-number effectiveness and is obtained from the reply data from certification data generation equipment 11. That is, the activation section 310 has 310g of program store sections which memorize the enciphered program, 310h of decode sections which read the enciphered program and are decoded using data K', code takeoff-connection 310i that takes out the decoded code, and 310f of code activation sections which perform the taken-out code.

[0157] The case where the activation means 310 is constituted as an application program which operates on a user's PC or a workstation is taken for an example, and a still more detailed configuration is described.

[0158] 310g of program store sections the enciphered program code is remembered to be is the storage region where it was specified in the computer.

[0159] 310f of code activation sections is CPU and OS of a computer.

[0160] 310g of program store sections can presuppose that it is a hard disk etc. a file space on an auxiliary storage unit. That is, the enciphered program code is memorized as a file.

[0161] The stereo of 310h of decode sections is a program code first performed in the activation means 310. 310h of decode sections can direct the address of 310g of program store sections in 310f of code activation sections directly and indirectly.

[0162] Where K' is given, when 310h of decode sections which are a program is started, 310h of decode sections The data memorized by 310g of program store sections are read for every block of order or the defined die length. Predetermined decode processing which used K' as the decode key is performed to the data, it orders 310f of code activation sections, and they are performed so that the decode result may be written out to the specific address of the program field on a computer. It means writing the result of having performed the predetermined decode algorithm in the specific location in a program field by using K' as a decode key to the encryption data memorized by 310g of program store sections by this processing.

[0163] Subsequently, 310h of decode sections orders 310f of code activation sections using a JMP instruction etc. to execute the run command of the specific address in a program field to which the program code which ordered to 310f of code activation sections, and was decoded was made to write out.

[0164] In this example of a configuration, if certification data are correctly generated by certification data generation equipment 11, the value after removing the random-number effectiveness will serve as a decode key for decoding correctly the enciphered program code which is memorized by 310g of program store sections. Using this decode key, 310h of decode sections decodes said encryption program code, and they order 310f of code activation sections to load the program code which it is as a result of decode to a program field, and to perform said loaded program code. Therefore, with the above-mentioned configuration, the program code decoded using the decode key decoded by the certification data generation means 11 will be performed following on the program code of 310h of decode sections (drawing 14).

[The third example]

[0165] In the third example in this invention, the access ticket t is data generated based on the following formula 16.

[Equation 16]

(16) t = D+F(n,e)

Each notation in an upper type expresses the following.

[0166] n is the product of the number p and q of the RSA methods, i.e., the two sufficiently big prime factors, (n=pq).

[0167] The user proper information e is a different number for every user, and it is used in order to identify a user.

[0168] phi (n) is the Euler number of n, i.e., the product of p-1 and q-1, (phi (n) = (p-1) (q-1)).

[0169] the access ticket private key D -- law -- it is a RSA private key under a number n, and a formula 17 is filled.

[Equation 17]

(17) gcd(D, phi (n)) =1 -- here, gcd (x y) expresses the greatest common measure of more than 2 [x] and y. The property expressed by the formula (17) guarantees that several E which fills a formula 18 exists.

[Equation 18]

(18) ED mod phi (n) = 1E is called an access ticket public key.

[0170] The 2 variable function F (x y) is a 2 variable function with which a function value cannot collide easily, for example, can be defined like a formula 19 using the above-mentioned one-way hash function h.

[Equation 19]

(19) F(x,y)=h(x | y)

With reference to drawing, the second example is further explained to a detail. Drawing 15 shows the configuration of the third example in this invention, and drawing 16 shows the flow of the data in drawing 15 . In drawing 15, certification data generation equipment 11 is constituted including the received-data storage section 111, the 1st operation part 112, the access ticket storage section 113, the 2nd operation part 114, the user proper information storage section 115, the certification data generation section 116, and the characteristic generation section 130. Certification data verification equipment 10 can adopt the configuration of the first example (drawing 3) or the second example (drawing 5). Here, explanation is not repeated.

[0171] The actuation in this configuration is explained below.

1. When a user accesses, certification data verification equipment 10 is started.

[0172] It is not different from the case of the first and the second example for the server

program on the server connected through PC, workstation, and network of the application program and user who operate on a user's PC or a workstation or all of the equipment of dedication like an IC card reader writer to be possible as the implementation approach of certification data verification equipment 10.

[0173] 2. the law of the RSA cryptograph certification data verification equipment 10 is remembered to be by the data C for authentication, and the access ticket public key storage section 101 -- write a group with a number n in the received-data storage section 111 in certification data generation equipment 11.

[0174] Since both the approach stated in the first example and the approach stated in the second example are applicable as a generation method of C, it does not limit especially here. C generated by said one of approaches shall be written in the received-data storage section 111 in certification data generation equipment 11.

[0175] 3. the RSA method which the 1st operation part 112 in certification data generation equipment 11 acquired the access ticket t memorized by the access ticket storage section 113, and was written in the received-data storage section 111 -- perform a formula 20 by the several n basis, and obtain middle information R'.

[Equation 20] (20) R'=Ct mod n [0176] 4. The characteristic generation section 130 in certification data generation equipment 11 acquires a user's proper information e memorized by the user proper information storage section 115, and performs count of a formula 21.

[Equation 21] (21) F(n,e)

[0177] 5. the data with which the 2nd operation part 114 in certification data generation equipment 11 was generated in the characteristic generation section 130 -- using -- count of a formula 22 -- performing -- difference -- acquire Information S.

[Equation 22] (22) S=CF (n, e) mod The certification data generation section 116 in n6. certification data generation equipment 11 obtains R' and S from the 1st and 2nd operation part 112 and 114, calculates a formula 23 and obtains R.

[Equation 23] (23) R=R'S -1 mod n, however S-1 -- law -- the inverse number of S under n, i.e., the number which fills a formula 24, is expressed.

[Equation 24] (24) S-S -1 mod n= 1 [0178] 7. Certification data generation equipment 11 returns R to the received-data storage section 105 of certification data verification equipment 10.

[0179] 8. Although the certification data received from certification data generation equipment 11 are verified with certification data verification equipment 10, the verification approach changes with generation methods of C which is some data for authentication.

[0180] If C is generated based on the approach of the first example, the verification will be performed according to the approach stated to the first example.

[0181] If C is generated based on the approach of the second example, the verification will be performed according to the approach stated to the second example.

[The fourth example]

[0182] The case where it is constituted from the fourth example by the portable operation means of the IC card with which a user's PC, the program on a workstation and said PC, or a workstation is equipped with certification data generation equipment, or a PC card (PCMCIA card) in the first thru/or the third example is described.

[0183] In the certification data generation equipment 11 of the first thru/or the third example, the user proper information e is confidential information, and attention must be paid [not revealing outside and]. Moreover, when actuation of the 2nd operation part 114 which performs count using the user proper information e is observed, there is risk of the user proper information e being revealed. It is also the same as when the computation of the function F in the third example (x y) is observed. That is, in order to prevent leakage of the user proper information e, it must prevent that the interior of the user proper information storage section 115, the 2nd operation part 114, and the characteristic generation section 130 is observed from the outside. In order to attain this purpose, it is effective if some certification data generation equipments 11 are constituted as hardware.

[0184] If the means which has portability like an IC card and a PC card as such hardware will be used, a user's convenience can be raised further. Parts peculiar to a user among certification data generation equipment are only the user proper information storage section and the access ticket storage section. Therefore, for example, the user proper information storage section 115 and the access ticket storage section 113, If the 2nd operation part 114 and the characteristic generation section 130 will be constituted in an IC card and a PC card and it will constitute as a program which operates on PC with which a user uses the remaining part of certification data generation equipment, or a workstation A part peculiar to each user will be realized among certification data generation equipment 11 as the IC card and a PC card which each user can carry, and the intersection independent of a user will be constituted common to PC or the workstation of arbitration as a program. It becomes possible only by every user equipping with his own IC card and PC card PC or the workstation of arbitration by which it was installed in said program by such configuration to use this PC or a workstation as certification data generation equipment for oneself.

[0185] Now, hardware with the special configuration for preventing data and the

program which were stored in the internal memory being observed from the outside, or being altered is called tamper-proof hardware (tamper REJISUTANTO hardware). As construction of tamper-proof hardware, patent No. 1863953, patent No. 1860463, JP,3-100753,A, etc. are known, for example.

[0186] In patent No. 1863953, the envelopment object which consists of two or more cards which have various kinds of conductor patterns in the perimeter of an information storage medium is established. Storage information is destroyed when it differs from the pattern with which the conductor pattern detected is predicted.

[0187] patent No. 1860463 -- setting -- the perimeter of an information storage medium -- a conductor -- while forming a coil, it is preparing the detecting circuit which consists of an integrating circuit etc., and when invasion to an electronic-circuitry field is, fluctuation of electromagnetic energy is detected and storage information is destroyed.

[0188] In JP,3-100753,A, an optical detector is prepared in the interior of hardware, an optical detector detects the outdoor daylight which enters when the force is applied and destroyed by hardware and it is punched, and a storage destructor resets storage information.

[0189] The further convenience to a user can be offered by realizing such tamper-proof hardware as an arithmetic unit in which a cellular phone like an IC card or a PC card (PCMCIA card) is possible.

[0190] Moreover, the microcontroller mounted in an IC card is supposed that it has high density assembly, therefore a tamper-proof property considerable at itself.

[0191] a user proper information storage means 115 by which drawing 17 holds the user proper information e in the first and the second example, and difference -- a second operation means 114 to generate information shows the configuration enclosed with tamper-proof hardware 160 like an IC card.

[0192] the user proper information storage section 115 in which drawing 18 holds the user proper information e in the third example, and difference -- the 2nd operation part 114 which generates information -- in addition, the configuration in which the characteristic generation section 130 is also enclosed with the tamper-proof hardware 161 is shown.

[0193] The IC card side I/F section 141 is an IC card side interface which manages the communication link of an IC card with a host, and, specifically, consists of a communication buffer and a communications program. The remaining part of the certification data generation equipment is constituted as a program which operates on a user's PC or a workstation. Since an operation of each means in the tamper-proof hardware 161 is as having stated to the first thru/or the third example, below, an

operation of the part is not explained. Moreover, although tamper-proof hardware is assumed to be what is an IC card in order to give explanation simple, this assumption does not restrict the generality of this invention at all. Drawing 19 shows the flow of the data in drawing 17 and drawing 18 .

[0194] Below, actuation is explained.

1. When a user accesses, certification data verification equipment 10 is started.

[0195] 2. the law of the RSA cryptograph certification data verification equipment 10 is remembered to be by the data C for authentication, and the access ticket public key storage section 101 -- write a group with a number n in the received-data storage section 111 in certification data generation equipment 11.

[0196] 3. The host side interface section 140 in certification data generation equipment 11 hands over the data C and n for authentication written in the received-data storage section 111 in the IC card side interface section 141. The host side interface section 140 manages the data communication between a host and an IC card in harmony with the IC card side interface section 141 prepared into the IC card.

[0197] 4. The access ticket retrieval section 142 searches and acquires the access ticket t memorized by the access ticket storage section 113 as a key of retrieval of the number n of the RSA methods.

[0198] 5. The 1st operation part 112 performs a formula 25 under the number n of the RSA methods written in the received-data storage section 111, and obtains middle information R'.

[Equation 25] (25) R'=Ct mod n [0199] 6. subsequently, the host side interface section 140 -- the IC card side interface section 141 -- a command -- publishing -- as the return value -- difference -- acquire Information S.

[0200] the case where the means in an access ticket and an IC card is based on the first or the second example, and is constituted -- difference -- Information S is a value calculated by the formula 26.

[Equation 26] (26) S=Ce mod n [0201] the case where the means in an access ticket and an IC card is based on the third example, and is constituted -- difference -- Information S is a value calculated by the formula 27.

[Equation 27] (27) S=CF (n, e) mod When R' and S are obtained from the 1st and 2nd operation part 112 and 114, it is based on the first and the second example and the certification data generation section 116 in n7. certification data generation equipment 11 is based on a formula 28 and the third example, it calculates a formula 29 and obtains R.

[Equation 28] (28) R=R'S mod n -- [Equation 29] (29) R=R'S -1 mod n [0202] 8.

Certification data generation equipment 11 returns R to the received-data storage section 105 of certification data verification equipment 10.

[0203] the above-mentioned operation -- setting -- middle information R' and difference -- since count of Information S is performed by juxtaposition by the IC card side which contains a calculation function the host side who is a user's PC or workstation -- the certification data generation means 11 -- the data C for authentication, and law -- the execution time after receiving a number n until it calculates the certification data R can be shortened, and, therefore, processing effectiveness is raised.

[0204] In this example, since those numbers n of the RSA methods differ if access tickets differ although two or more access tickets are memorized by the access ticket storage section 113, by using n as a key, it matches with n and an access ticket is remembered that retrieval is possible.

[0205] Moreover, it is a base that the numbers n of the RSA methods which application and a server use for an access control differ for every application or server.

[0206] The access ticket retrieval section 142 searches a suitable access ticket by using as a key the number n of the RSA methods given from certification data verification equipment 10, and presents generation of future certification data with it. By this retrieval function, certification data generation equipment 11 becomes possible [calculating and returning suitable certification data according to the accessed object (the application according to individual, and server according to individual)], without forcing a burden upon a user in any way.

[0207] [the fifth example] -- in the fifth example in this invention, a Pohlig-Hellman unsymmetrical key code is used instead of the RSA public key encryption used in the third example.

[0208] a Pohlig-Hellman unsymmetrical key code -- law -- the point using the big prime factor p as a number -- it is -- law -- different outside from the RSA public key encryption using the product n of the two prime factors (= pq) as a number is the same cipher system as RSA public key encryption. however -- RSA public key encryption -- one key E and law -- it was possible to have used D as an individual being secret from a number n, using E and n as a public key, since it was very difficult to calculate another key D. On the other hand, in a Pohlig-Hellman unsymmetrical key code code, from E and p, since D is easily calculable, E and p cannot be used as a public key. That is, it is necessary to make both E and D secret [between persons concerned], and the same use gestalt as a common key encryptosystem like DES (Data Encryption Standard) must be taken.

[0209] In this example, the access ticket t is data generated based on the following formula 30.

[Equation 30]

(30) t = D+F(p,e)

Each notation in an upper type expresses the following.

[0210] p is the sufficiently big prime factor.

[0211] The user proper information e is a different number for every user, and it is used in order to identify a user.

[0212] the access ticket private key D -- law -- on the other hand, the key of the Pohlig-Hellman code under a number p comes out, it is and a formula 31 is filled.

[Equation 31]

(31) gcd(D, p-1) =1 -- here, gcd (x y) expresses the greatest common measure of more than 2 [x] and y.

[0213] The property expressed by the formula 31 guarantees that several E which fills a formula 32 exists.

[Equation 32]

(32) ED mod p-1 = 1 [0214] The 2 variable function F (x y) is a 2 variable function with which a function value cannot collide easily, for example, can be defined like a formula 33 using the above-mentioned one-way hash function h.

[Equation 33]

(33) F(x,y)=h(x|y)

Below, with reference to drawing 20 and drawing 21 , the fifth example is further explained to a detail. Drawing 20 shows the configuration of the fifth example and drawing 21 shows the flow of the data in drawing 20 . In drawing 20, certification data verification equipment 20 is constituted including the key storage section 401, the random-number-generation section 402, the random-number storage section 403, the received-data storage section 405, the random-number-ized section 421, the ** data storage section 422 for authentication, the random-number effectiveness removal section 423, and the activation means 310. Moreover, the certification data generation section 41 is constituted including the received-data storage section 411, the 1st operation part 412, the access ticket storage section 413, the 2nd operation part 414, the user proper information storage section 415, the certification data generation section 416, and the characteristic generation section 430.

[0215] Below, actuation is explained.

1. When a user accesses, certification data verification equipment 40 is started.

[0216] 2. the law certification data verification equipment 40 is remembered to be by the data C for authentication, and the key storage section 401 -- write a group with a number p in the received-data storage section 411 in certification data generation

equipment 41.

[0217] Although based on the approach which applied to the approach stated in the second example correspondingly as a generation method of C in this example, it is not difficult to constitute the approach according to the approach stated in the first example, either.

[0218] the law currently held in the random number r among certification data verification equipment by the random-number-generation section 402 of 40 at the key storage section 401 -- it generates so that it may become a number p and relatively prime, and it records on the random-number storage section 403. the random-number-ized section 421 is stored in the key storage section 401 -- having -- **** -- a characteristic E and law -- a formula 34 is calculated by acquiring a number p and acquiring data C' further memorized by the ** data storage section 422 for authentication.

[Equation 34] (34) C=rEC' mod p -- here, ** data C' for authentication is the value which was generated so that relational expression 35 might be filled to Data K, and was stored in the ** data storage section 305 for authentication.

[Equation 35] (35) C'=KE mod p [0219] 3. The 1st operation part 412 in certification data generation equipment 41 acquires the access ticket t memorized by the access ticket storage section 413, performs a formula 36 under the number p of the RSA methods written in the received-data storage section 411, and obtains middle information R'.

[Equation 36] (36) R'=Ct mod p [0220] 4. The characteristic generation section 430 in certification data generation equipment 41 acquires a user's proper information e memorized by the user proper information storage section 415, and performs count of a formula 37.

[Equation 37] (37) F(p,e)

[0221] 5. the data with which the 2nd operation part 414 in certification data generation equipment 11 was generated in the characteristic generation section 430 -- using -- count of a formula 38 -- performing -- difference -- acquire Information S.

[Equation 38] (38) S=CF (p, e) mod The certification data generation section 416 in p6. certification data generation equipment 41 obtains R' and S from the 1st and 2nd operation part 412 and 414, calculates a formula 39 and obtains R.

[Equation 39] (39) R=R'S -1 mod p, however S-1 -- law -- the inverse number of S under p, i.e., the number which fills a formula 40, is expressed.

[Equation 40] (40) SS-1 mod p = 1 [0222] 7. Certification data generation equipment 41 returns R to the received-data storage section 405 of certification data verification

equipment 40.

[0223] 8. The random-number effectiveness removal section 423 in certification data verification equipment 10 takes out the random number r previously generated out of the random-number storage section 403, and calculates a formula 41.

[Equation 41] (41) K' -- the combination of the first proper information e of the access ticket t used in =r-1R mod p certification data generation equipment 41, and a user -- a right case -- as long as -- note that K' obtained as a result of count and K are in agreement.

[The sixth example]

[0224] The sixth example of this invention shows the example of a configuration which used ElGamal public key encryption instead of the RSA public key encryption in the third example.

[0225] In the sixth example in this invention, the access ticket t is data generated based on the following formula 42.

[Equation 42]

(42) t = X+F(p,e)

Each notation in an upper type expresses the following.

[0226] p is the sufficiently big prime factor.

[0227] The user proper information e is a different number for every user, and it is used in order to identify a user.

[0228] the access ticket private key X -- law -- it is the private key of the ElGamal cryptosystem under a number p, and suppose that it is Y a corresponding public key. That is, a formula 43 is filled.

[Equation 43] (43) Y = aX mod p -- here, a fills the generator 44 and 45 of the multiplicative group of the finite field of order p, i.e., formulas.

[Equation 44] (44) a != 0 -- [Equation 45]

(45) min {x>0 | ax=1 mod p} = p-1 and Y are called an access ticket public key.

[0229] The 2 variable function F (x y) is a 2 variable function with which a function value cannot collide easily, for example, can be defined like a formula 46 using the above-mentioned one-way hash function h.

[Equation 46]

(46) F(x,y)=h(x | y)

Below, with reference to drawing 22 and drawing 23 , the sixth example is explained further. Drawing 22 shows the configuration of the sixth example and drawing 23 shows the flow of the data in the sixth example. In drawing 22, certification data verification equipment 50 is constituted including the access ticket public key storage section 501,

the random-number-generation section 502, the random-number storage section 503, the received-data storage section 505, the random-number-ized section 521, the ** data storage section 522 for authentication, the random-number effectiveness removal section 523, and the activation means 310. The certification data generation section 51 is constituted including the received-data storage section 511, the 1st operation part 512, the access ticket storage section 513, the 2nd operation part 514, the user proper information storage section 515, the certification data generation section 516, and the characteristic generation section 530.

[0230] Actuation is explained below.

1. When a user accesses, certification data verification equipment 50 is started.

[0231] 2. the law by which certification data verification equipment 50 is remembered to be the groups u and C of the data for authentication by the access ticket public key storage section 501 -- write a number p in the received-data storage section 511 in certification data generation equipment 51.

[0232] Although u and C' are memorized as ** data for authentication by the ** data storage section 522 for authentication, they fulfill the following property.

[0233] u -- Above a -- law -- it is the number which made the suitable random number z the characteristic and carried out the exponentiation under p, namely, a formula 47 is filled.

[Equation 47] (47) u = az mod p [0234] C' -- the access ticket public key Y -- law -- it is the basis of p, and it is the number which made the above-mentioned random number z the characteristic, and carried out the exponentiation, and a product with the suitable data K, and a formula 48 is filled.

[Equation 48] (48) C'=YzK mod p [0235] The data C for authentication are generated as follows.

[0236] the law by which certification data verification equipment 50 is held by the random-number-generation section 502 in the random number r at the access ticket public key storage section 501 -- it generates so that it may become a number p and relatively prime, and it records on the random-number storage section 503.

[0237] Subsequently, the random-number-ized section 521 calculates a formula 49 by acquiring data C' memorized by the ** data storage section 522 for authentication.

[Equation 49] (49) C=rC' mod p [0238] 3. the law which the 1st operation part 512 in certification data generation equipment 51 acquired the access ticket t memorized by the access ticket storage section 513, and was written in the received-data storage section 511 -- perform a formula 50 under a number p and acquire the middle information S.

[Equation 50] (50) S = ut mod p [0239] 4. The characteristic generation section 530 in certification data generation equipment 51 acquires a user's proper information e memorized by the user proper information storage section 515, and performs count of a formula 51.

[Equation 51]

(51) F(p,e)

[0240] 5. the data with which the 2nd operation part 514 in certification data generation equipment 51 was generated in the characteristic generation section 530 -- using -- count of a formula 52 -- performing -- difference -- obtain information S'.

[Equation 52]

(52) S' = uF (p, e) mod p [0241] 6. The certification data generation section 516 in certification data generation equipment 51 obtains S and S' from the 1st and 2nd operation part 512 and 514, calculates a formula 53 and obtains R.

[Equation 53]

(53) R = S-1 S'C mod p, however S-1 -- law -- the inverse number of S under p, i.e., the number which fills a formula 54, is expressed.

[Equation 54] (54) SS-1 mod p = 1 [0242] 7. Certification data generation equipment 51 returns R to the received-data storage section 505 of certification data verification equipment 50.

[0243] 8. The random-number effectiveness removal section 523 in certification data verification equipment 10 takes out the random number r previously generated out of the random-number storage section 503, and calculates a formula 55.

[Equation 55] (55) K' -- the combination of the proper information e of the access ticket t used in =r-1R mod p certification data generation equipment 51, and a user -- a right case -- as long as -- note that K' obtained as a result of count and K are in agreement. Now, when the above-mentioned gestalt is carried out directly, the following problems arise. That is, it becomes possible by applying the same ** data u for authentication and same C' to the access rating authentication procedure of multiple times to constitute the equipment which copies an operation of certification data generation equipment 11 without user proper information or an access ticket. From the ** data C for authentication published from certification data verification equipment 10 in a first-time authentication procedure, and the certification data R which certification data generation equipment 11 generates to first, H=RC -1 mod p is calculated. This H is recorded on imitation equipment instead of user proper information and an access ticket. Imitation equipment is formula R=HC to the ** data for authentication of arbitration (u, C) which certification data verification equipment 10 publishes. mod What is necessary

is to generate the certification data R according to p, and just to make it return to certification data verification equipment 10. As an approach of coping with this attack, only the required number memorizes the group u of the ** data for authentication, and C' in the ** data storage section 522 for authentication, and how to make it throwing away at every authentication procedure can be considered. It is made mutually different [the random number z used for the generation] by the ** data for authentication which are different from each other here. u is u=ak. Although it defines as modp, please care about that k was a random number.

[The seventh example]

[0244] In the seventh example of this invention, the example of a configuration using the signature key of an ElGamal signature is described as description information on access rating authentication.

[0245] In the seventh example in this invention, the access ticket t is data generated based on a formula 56.

[Equation 56]

(56) t = X+F(p,e)

Each notation in an upper type expresses the following.

[0246] p is the sufficiently big prime factor.

[0247] The user proper information e is a different number for every user, and it is used in order to identify a user.

[0248] the access ticket private key X -- law -- it is the signature key of the ElGamal signature by the basis of a number p, and suppose that it is Y a corresponding public key. That is, a formula 57 is filled.

[Equation 57]

(57) Y = aX mod p -- here, a fills the generator 58 and 59 of the multiplicative group of the finite field of order p, i.e., formulas.

[Equation 58] (58) a != 0 -- [Equation 59]

(59) min {x>0 | ax=1 mod p} = p-1 and Y are called an access ticket public key.

[0249] The 2 variable function F (x y) is a 2 variable function with which a function value cannot collide easily, for example, can be defined like a formula 60 using the above-mentioned one-way hash function h.

[Equation 60]

(60) F(x,y)=h(x | y)

[0250] With reference to drawing 24 and drawing 25 , the seventh example is explained further below. Drawing 24 shows the configuration of the seventh example and drawing 25 shows the flow of the data in the seventh example. In drawing 24, certification data

verification equipment 60 is constituted including the access ticket public key storage section 601, the random-number-generation section 602, the random-number storage section 603, the received-data storage section 605, the verification section 606, the activation section 607, and the error-processing section 608. Moreover, certification data generation equipment 61 is constituted including the received-data storage section 611, the random-number-generation section 612, the 1st operation part 613, the 2nd operation part 614, the access ticket storage section 615, and the user proper information storage section 616. Actuation is explained below.

1. When a user accesses, certification data verification equipment 60 is started.

[0251] 2. the law certification data verification equipment 60 is remembered to be by the data C for authentication, and the access ticket public key storage section 601 -- write a number p and Generator a in the received-data storage section 611 in certification data generation equipment 61. The data C for authentication are generated as follows.

[0252] the law by which certification data verification equipment 60 is held by the random-number-generation section 602 in the random number r at the access ticket public key storage section 601 -- while it generates so that it may become a number p and relatively prime, and recording said r on the random-number storage section 603, it considers as the data C for authentication (C=r).

[0253] 3. the random-number generation section 612 in certification data generation equipment 61 -- law -- generate a p-1 number and the random number k which is relatively prime.

[0254] the law by which the 1st operation part 613 was written in said random number k and the received-data storage section 611 -- the first certification data R is calculated from a number p and Generator a according to a formula 61.

[Equation 61] (61) $R = ak \bmod p$ [0255] the user proper information e memorized by the access ticket t and the user proper information storage section 616 the 2nd operation part 614 is remembered to be by the access ticket storage section 615, said random number k, the first [said] certification data R and the data C for authentication written in the received-data storage section 611, and law -- the second certification data S is calculated from a number p according to a formula 62.

[Equation 62]

(62) $S = (C-R(t-F(p, e)))\ k-1 \bmod p-1$ [0256] 4. Certification data generation equipment 61 returns R and S which are the first and second certification data to the received-data storage section 605 of certification data verification equipment 60.

[0257] 5. The verification section 606 in certification data verification equipment 60 takes out Y and p which are memorized by the random number r (= C) and the access

ticket public key storage section 601 which are memorized by the random-number storage section 603, and verifies the certification data R and S by the formula 63.

[Equation 63] (63) ar = YRRS mod p [the eighth example]

[0258] The eighth example of this invention describes the generation method of an access ticket.

[0259] The count based on a secret number is required for generation of the access ticket in the first thru/or the seventh example. Therefore, the secret number used for count needs to be revealed, or generation of an access ticket needs to be performed with safe equipment without a fear of being exposed of the intermediate result of count.

[0260] The easiest approach for constituting such safe equipment is building the server which provides a user with access ticket issue service on PC which a user's uses, or a computer independent of a workstation. A server generates an access ticket according to the demand from a user. The computational procedure of a secret number and an access ticket is protected by constituting in the configuration of a server, so that the invasion from the outside may be intercepted.

[0261] For example, it becomes possible to intercept the invasion from the outside by being locked and constituting an access ticket issue server on the computer of the individual interior of a room by which receipts and payments are managed severely.

[0262] Moreover, in order to raise a user's convenience, it is also possible to connect said access ticket issue server to a network, and to constitute the access ticket issue demand from a user through a network, so that reception and the generated access ticket may be too delivered to a user through a network.

[0263] Thus, when connecting an access ticket issue server to a network, it needs to be built so that safety may fully be maintained also to the invasion from the outside through a network using a fire wall technique (D. refer to Brent Chapman & Elizabeth D. Zwicky, Building Internet Firewalls, O'Reilly & Associates, Inc. or the Japanese translation, fire wall construction, and O'Reilly Japan).

[0264] The access ticket in the first thru/or the seventh example is generated in the format which cannot be used in addition to the just user (user holding the user proper information e that it used when calculating an access ticket).

[0265] The access ticket in the first thru/or the seventh example is generated by the basis of a still stricter safety standard. That is, even if the user who tries unjust access did not ask for him or those for others but collected the access tickets of the arbitration number, it is impossible to constitute the equipment imitating actuation of the certification data generation equipment which forged another access ticket from there, or was stated in the first thru/or the fifth example.

[0266] It also becomes possible comparatively from the safety of the above access tickets to deliver to a user using a delivery means with low safety like an electronic mail about the access ticket which the access ticket issue server generated.

[The ninth example]

[0267] This example describes the proper information of a different user from the first thru/or the seventh example, and the construction of an access ticket. The description of this configuration approach is that it does not need confidential information for generation of an access ticket.

[0268] Therefore, the access ticket issue server built by insurance on the occasion of access ticket generation to the invasion from the outside which was stated in the eighth example is unnecessary. A user can generate an access ticket freely by the program which operates on PC to own or a workstation. In a program, neither a secret constant nor a secret procedure exists, and even if it analyzes a program, it cannot take out any information which makes unlawful access possible.

[0269] User's U proper information is the individual key d of a RSA public key pair. The public key corresponding to this user's proper information is set to (eU, nU). That is, it is the integer which is nU=pUqU and was determined that dU and eU will fill relational expression 64 to the two different large prime factors pU and qU.

[Equation 64]

1<=dU<= (pU-1) (qU-1)

(64) 1<=eU<= (pU-1) (qU-1)

eUdU**1 mod (pU-1) (qU-1)

Here, nU adds the conditions of being more than the constant N shared by all users.

[0270] The access ticket to User U is constituted as follows.

[0271] The public key (E, n) of a RSA public key pair is used as the public key of an access ticket, and this public key and the private key which makes a pair are set to D. When making factorization in prime numbers of n into n=pq, relational expression 65 is realized.

[Equation 65]

$$(65) \quad 1 \leq D < N$$
$$DE \equiv 1 \mod (p-1)(q-1)$$

The access ticket tU is [Equation 66] defined by the formula 66. (66) tU=DeU mod nU

[0272] The description information on the access rating authentication in this example is the individual key D of said RSA public key pair.

[0273] The certification data generation equipment 11 in this example proves that right

certification data can be calculated through the communication link with certification data verification equipment 10 like the case of the first thru/or the seventh example corresponding to the ability to know the description information on access rating authentication, i.e., the given data for authentication.

[0274] The data which encipher D which is the description information on access rating authentication, and are obtained are an access ticket, and the description of this example is that it is the only decode key for a user's proper information to solve this encryption. Furthermore, if it says, any number of persons who can know a corresponding public key from the place which is using a user's proper information as the individual key of RSA public key encryption are in the point which can generate an access ticket. Below, the operation in this example is described with reference to drawing 26 .

[0275] 1. Certification data verification equipment 10 writes the data C for authentication in the received-data storage section 711 of certification data generation equipment 10.

[0276] 2. The decode key generation section 712 of certification data generation equipment 11 acquires the access ticket tU remembered to be a user's proper information dU memorized in the user proper information storage section 715 in the access ticket storage section 713, and calculates D' based on a formula 67.

[Equation 67] (67) The D'=tU dU mod nU3. certification data generation section 714 calculates a formula 68 by considering as an input the data C for authentication remembered to be said D' generated by the decode key generation section 712 by the received-data storage section 711, and asks for R. The certification data generation section 714 transmits to certification data verification equipment by using a count result as reply data.

[Equation 68] (68) R= CD' mod n [0277] 4. Certification data verification equipment verifies the justification of the certification data R.

[0278] Access ticket tU=DeU mod Since the private key D of the access ticket in nU must be kept secret also to User U, the user proper information storage section 713, the decode key generation section 712, and the certification data generation section 714 are enclosed into a defense means 760 to have a tamper-proof property, among the equipment configurations of the above-mentioned certification data generation equipment 11.

[0279] It restricts, as well as the case of the 1st thru/or the seventh example when a user's first proper information and the right combination of an access ticket are used by certification data generation equipment 11, and the certification data R generated by

certification data generation equipment are correctly verified by certification data verification equipment.

[0280] [the tenth example] -- the tenth example of this invention A symmetry key code is used for count of the certification data in certification data generation equipment instead of public key encryption (RSA cryptograph). If an access ticket removes the point which is data which encipher the decode key (the same as that of an encryption key) D of said symmetry key code with the public key (eU, nU) corresponding to the individual key of the RSA public key pair which is user proper information, and are obtained, it is almost the same as the ninth example.

[0281] That is, when the encryption function of a symmetry key code is expressed as Encrypt (a key, plaintext) (an output is a cipher) and a decode function is expressed as Decrypt (a key, cipher) (an output is a plaintext), the protected certification data C are defined by the formula 69.

[Equation 69]

(69) C=Encrypt(D,K)

Furthermore, the access ticket tU is [Equation 70] defined by the formula 70. (70) tU=DeU mod The equipment configuration of certification data generation equipment and an operation are explained based on drawing 26 R> 6 below nU.

[0282] 1. Certification data verification equipment 10 writes the data C for authentication in the received-data storage section 711 of certification data generation equipment 10.

[0283] 2. The decode key generation section 712 of certification data generation equipment 11 acquires the access ticket tU remembered to be a user's proper information dU memorized in the user proper information storage section 715 in the access ticket storage section 713, and calculates D' by the formula 71. A count result is outputted to the certification data generation section 714.

[Equation 71] (71) D'=tU dU mod nU [0311] 3. The certification data generation section 714 calculates a formula 72 by considering as an input the data C for authentication remembered to be D' obtained from the decode key generation section 712 by the received-data storage section 711, and asks for R. A count result is transmitted to certification data verification equipment 10 as reply data.

[Equation 72]

(72) R=Decrypt(D',C)

[0284] 4. Determine whether to perform whether processing of normal is continued by verifying R, and error processing among certification data verification equipment 11.

[Effect of Example(s)] -- when the above-mentioned example is carried out for the

purpose of the access control (execution control) to the application program performed on a user's PC or a workstation so that clearly from the above explanation, the effectiveness described below can be offered.

[0285] 1. A user should just hold user proper information for even free to a proper.

[0286] 2. Perform protection processing to a program by the unrelated approach with user proper information at application creation time.

[0287] 3. An access ticket is published by the authorized user in activation of application, and the activation of application of this user is attained only by holding one's user proper information and access ticket.

[0288] 4. Though the user who is not the owner of normal holds it, by it, if activation of application is possible for an access ticket, it is the approach which is not, and is generated by insurance.

[0289] Even when distributing the hardware which built in user proper information to a user according to these descriptions, what is necessary will be for distribution to be managed at once for every user, and for a programmer to be concerned with whether the program of the place to create is used by whom, and for there to be nothing and just to perform protection processing of one application by the general approach. Therefore, the trouble which must change the protection approach of a program for every user that O user proper information must be set up for every application, therefore hardware must be mailed to a user for every application is solved, and it contributes to reduction of cost, and improvement in convenience sharply so that different user proper information for every O user which was the trouble of the conventional technique may be identified.

[0290] According to the above-mentioned example, although an access ticket is needed for activation of an application program, since an access ticket is safe digital information available only to the user of normal, it can be delivered to a user simple through a network etc.

[0291] Moreover, whenever a user changes the application program to be used, he needs to exchange an access ticket, but as mentioned above, since an access ticket is digital information, the program in a computer can perform replacement actuation easily. That is, the conventional complicatedness that a user has to exchange hardware whenever it changes an application program is canceled.

[0292] furthermore, the time of holding all the access tickets of the combination of O specification which sets up a different right of activation for every part of O application program, since it is possible to arrange freely the certification data verification equipment (procedure) based on different certification data in the location of the arbitration in an application program in the above-mentioned example -- as long as -- a

fine access control [say / granting the right of activation] is realizable with execution control.

[0293] In addition, it is clear that this invention's it is not limited to program execution control and this invention can be applied to the access control to privacy protection, file, and computer resource of e-mail. That is, access of a file etc. is controllable if the authentication technique of this invention is applied to the device in which a file, mail, and a computer resource are managed.

[0294]

[Effect of the Invention] It will end, if the description information and user proper information on access rating authentication can be made to become independent, therefore the protection side and user side also prepares one proper information by introducing the auxiliary data for certification (access ticket) according to this invention, as explained above. An access ticket is data calculated based on specific user proper information and the description information on access rating authentication, and it is impossible in computational complexity at least to calculate the description information on access rating authentication for user proper information from an access ticket to not knowing. And data ** for right certification is calculated only within the case where the right combination of user proper information and an access ticket, i.e., the combination of the access ticket calculated based on user proper information and this user proper information, is inputted. Therefore, access rating of users, such as execution control, can be attested by a user's possessing user proper information beforehand, and protection persons', such as a programmer's, preparing the description information on access rating authentication independently of the user proper information which a user possesses, and creating an access ticket according to a user's proper information and the description information on access rating authentication used for creation of an application program etc., and distributing.

[Brief Description of the Drawings]

[Drawing 1] It is the block diagram showing the theoretic example of a configuration of this invention.

[Drawing 2] It is the block diagram showing the configuration of the first example of this invention.

[Drawing 3] It is the block diagram showing the configuration of the certification data verification equipment of the first example, and certification data generation equipment.

[Drawing 4] It is a flow Fig. explaining actuation of the first example.

[Drawing 5]It is the block diagram showing the configuration of the certification data

verification equipment of the second example, and certification data generation equipment.

[Drawing 6] It is a flow Fig. explaining actuation of the certification data verification equipment of the second example.

[Drawing 7]It is the block diagram showing the example of a configuration of the activation section of the certification data verification equipment of the second example.

[Drawing 8] It is a flow Fig. explaining actuation of the example of a configuration of the activation section of drawing 7 .

[Drawing 9]It is the block diagram showing other examples of a configuration of the activation section of the certification data verification equipment of the second example.

[Drawing 10] It is a flow Fig. explaining actuation of the example of a configuration of the activation section of drawing 9 .

[Drawing 11]It is the block diagram showing other examples of a configuration of the activation section of the certification data verification equipment of the second example.

[Drawing 12] It is a flow Fig. explaining actuation of the example of a configuration of the activation section of drawing 11 .

[Drawing 13]It is the block diagram showing other examples of a configuration of the activation section of the certification data verification equipment of the second example.

[Drawing 14] It is a flow Fig. explaining actuation of the example of a configuration of the activation section of drawing 13 .

[Drawing 15]It is the block diagram showing the configuration of the certification data generation equipment of the third example of this invention.

[Drawing 16] It is a flow Fig. explaining actuation of the certification data generation equipment of the third example.

[Drawing 17] It is the block diagram showing the example of a configuration of the fourth example of this invention.

[Drawing 18] It is the block diagram showing other examples of a configuration of the fourth example of this invention.

[Drawing 19] It is a flow Fig. explaining actuation of drawing 17 .

[Drawing 20] It is the block diagram showing the configuration of the fifth example of this invention.

[Drawing 21] It is a flow Fig. explaining actuation of the data verification equipment of the fifth example.

[Drawing 22] It is the block diagram showing the configuration of the sixth example of this invention.

[Drawing 23] It is a flow Fig. explaining actuation of the sixth example.

[Drawing 24] It is the block diagram showing the configuration of the seventh example of this invention.

[Drawing 25] It is a flow Fig. explaining actuation of the seventh example. It is drawing explaining Challenge Handshake Authentication Protocol.

[Drawing 26] It is a block diagram explaining the authentication using the access ticket of the ninth example and the tenth example.

[Description of Notations]

10 Certification Data Verification Equipment

11 Certification Data Generation Equipment

12 Access Ticket Generation Equipment

13 Access Ticket

14 The Description Information on Access Rating Authentication

15 Verification Routine

16 User Proper Information

17 Certification Data Generator

20 Token (Protection Means)

101 Access Ticket Public Key Storage Section 101

102 Random-Number-Generation Section

103 Random-Number Storage Section

105 Received-Data Storage Section

106 Verification Section

107 Activation Section

108 Error-Processing Section

111 Received-Data Storage Section

112 1st Operation Part

113 Access Ticket Storage Section

114 2nd Operation Part

115 User Proper Information Storage Section

116 Certification Data Generation Section